

FEDERAL TRADE COMMISSION

I N D E X

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

WELCOMING REMARKS: PAGE:
BY TIMOTHY J. MURIS, CHAIRMAN, FTC 4

PRESENTER:
DICK CLARKE 10

PANEL: PAGE:
I 35
II 118
III 153
IV 190

FEDERAL TRADE COMMISSION

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

In the Matter of:)
CONSUMER INFORMATION SECURITY)
WORKSHOP)
-----)

MAY 20, 2002

Room 432
Federal Trade Commission
6th Street and Pennsylvania
Ave., NW
Washington, D.C. 20580

The above-entitled workshop was commenced,
pursuant to notice, at 9:05 a.m.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

P R O C E E D I N G S

MR. EICHORN: We're getting a little bit of a late start this morning ironically because of security downstairs, but we're ready now, so let's roll on.

I just have a few brief announcements. On the mundane side, in your packets you'll find order forms for sandwiches from the cafeteria upstairs. If you're interested in pre ordering a sandwich, you can fill out that form and pass it to the end of the room, find me or some other staff and hand us that form, and we'll make sure that you have a pre ordered sandwich.

Also, as many of you have already discovered, there's no coffee outside, but there is coffee upstairs on the seventh floor in the cafeteria, so if you need coffee at any point, it's right off the elevator bank.

Also I would ask that you all turn off your pagers and phone ringers just as a reminder.

In our workshop today, we're going to be having questions from the mike here at the end of each panel, so if there are people in the overflow rooms who want to ask questions, we ask that you come up to the room at the appropriate time in the panel. The moderator will indicate that people can come up for questions, so if

1 you're in 532 or 332, you might want to come up here.

2 Also, the record for this workshop is going to
3 be open for another month, until June 21st, so if
4 there's any comment that you want to get into the record
5 that you want to provide to us, we would be happy to
6 receive that. You can email those to us at Security
7 underlined Workshop at FTC.GOV.

8 At this point, it's my pleasure to introduce
9 Chairman Muris.

10 CHAIRMAN MURIS: Thank you very much, and
11 welcome to our workshop on consumer information
12 security. We're here today because information security
13 has become not just a business issue, but an important
14 consumer issue as well.

15 Computers are black boxes for most people.
16 Their workings are a mystery. Unfortunately, for too
17 many, that same sense of mystery extends to the threats
18 that exist. Too many consumers learn about security the
19 hard way, after they've set loose an email virus in their
20 system or their computer has been taken over and used in
21 a denial of service attack.

22 I want to thank you for coming to help educate
23 us on these issues. I especially want to thank our
24 panelists who traveled from near and far to be with us.

1 We've lined up an impressive groups of experts to
2 discuss the current state of consumer information
3 security, as well as new and emerging ways to improve
4 that security.

5 Because the audience will also ask questions, we
6 look forward to learning not only from the panelists,
7 but also from you.

8 I believe in the value of information. The
9 average American enjoys access to credit and financial
10 services, shopping choices and educational resources
11 that earlier Americans could never have imagined.

12 Today we can check our credit card and bank
13 balances over the phone 24 hours a day. We can order
14 books, clothes or gifts online while we are having our
15 first cup of coffee in the morning, or we can review our
16 finances in a convenient, consolidated statement
17 whenever we like.

18 Even with the decline in Internet stock prices,
19 the impact the Internet has had on our economy is hard
20 to overstate. The free flow of information that
21 computers and the Internet make possible is of enormous
22 value. We marvel at the ways that the computer and the
23 Internet have changed how Americans live, work and play.

24 With the enormous benefits have come new

1 challenges. Instead of lions, tigers and bears, there
2 are viruses, hackers and worms. The destruction theft
3 or disclosure of consumer's data are serious problems.
4 Sure, consumers use their computers to email jokes and
5 play Solitaire, but they also use them to store
6 sensitive information such as passwords, financial
7 records and health data.

8 Just cleaning up a virus infected computer can
9 be time consuming and expensive, and as ever more
10 powerful computers get hooked up to broadband Internet
11 connections, the potential consequences from security
12 incidents grow.

13 Consumers' security affects everybody. When
14 hackers harness many computers together to attack a
15 particular target, the operation of the network as a
16 whole is affected.

17 Many businesses, such as small ones without full
18 time systems administrators, face the same security
19 challenges that consumers do. Businesses as a whole
20 hold more information in their databases about consumers
21 than consumers hold themselves.

22 Thus, the security of businesses that maintain
23 consumer information, whether that information was
24 originated online or off, is an important consumer

1 issue. Businesses that transact with consumers online
2 have another reason to care about security. B-to-C
3 e-commerce would suffer if consumers were to lose
4 confidence that they can transact safely online.

5 To educate ourselves about these issues and to
6 see what role we might be able to play in encouraging
7 strong but workable security practices, last October I
8 publicly raised the idea of having a workshop on
9 security. Since then Commissioner Orson Swindle has
10 taken the leading role in making this workshop happen.

11 Many of you know that Commissioner Swindle has
12 been heading the U.S. delegation to the working group
13 that is advising the OECD security guidelines. Tomorrow
14 morning he will be speaking to you about that process.

15 Many substantive issues that the Commission is
16 currently working on involve security. For example, we
17 just issued a final rule to implement the safeguard
18 aspect of the Gramm-Leach-Bliley Act. The rule
19 requires, among other things, that financial
20 institutions covered by the rule establish and maintain
21 an information security program to protect their
22 consumers' personal information.

23 We expect to issue educational materials about
24 the rule for consumers and businesses very shortly.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 We're also working to reduce identity theft, which is
2 the leading source of complaints made to the
3 Commission's Consumer Sentinel database. If a database
4 holding consumer's personal information is not secure,
5 it is easier for a hacker or disloyal insider to gain
6 access to that information to steal someone's identity.
7 And we're working hard to make sure our own house is
8 order.

9 Here at the FTC, we've been going the extra
10 distance at all levels of the agency to put tighter
11 security procedures in place. Last month I sent a
12 memorandum to all of our staff stressing the importance
13 of information security to the Commission's mission and
14 launching a new security program.

15 We're upgrading our equipment and
16 infrastructure. We're developing security plans for all
17 major systems and applications. We're initiating
18 internal and external audits to assess our program.
19 We're strengthening password requirements. We're going
20 to be briefing all staff, not just IT personnel,
21 annually on computer risks and threats, and we'll be
22 teaching best practices for home computers. We believe
23 that practicing good security at home will carry over to
24 work.

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 These efforts parallel those being made all
2 across government agencies to make cyber security a
3 priority.

4 It's my great pleasure now to introduce the
5 person who is leading those efforts on behalf of the
6 administration.

7 Dick Clarke is the President's special advisor
8 on cyber security issues, and chairs the President's commission on
9 critical infrastructure protection. Like Tom Ridge, Dick has the
10 formidable task of coordinating numerous agency security efforts, as I
11 understand it, 23 different federal agencies.

12 I want to highlight just a couple of the issues
13 on which Dick is working. He's formulating the national
14 strategy for cyber security, a multi pronged strategy to
15 improve the security of government agencies, businesses
16 and consumers.

17 Another issue is consumer education. Dick's
18 team has been very active in working with the private
19 sector to get security information to consumers. Many
20 of the organizations involved in the effort are present
21 here today.

22 Before his appointment as special advisor to the
23 President, Dick served as national coordinator for
24 security infrastructure protection and counter-terrorism

1 on the National Security Council. As national
2 coordinator, he led the U.S. government's efforts on
3 counter-terrorism, cyber security, continuity of
4 government operations, domestic preparedness for weapons
5 of mass destruction and international organized crimes.

6 In the George H. W. Bush Administration, Dick
7 was the assistant secretary of state for political
8 military affairs. In that capacity, he coordinated
9 State Department support for Desert Storm and led efforts
10 to create post war security architecture.

11 In 1992, General Scowcroft appointed Mr. Clarke
12 to the National Security Council staff. He continued as
13 a member of that staff throughout the Clinton
14 Administration.

15 In the Reagan Administration, Dick was the
16 deputy assistant secretary of state for intelligence.

17 Dick's a career member of the senior executive
18 service and began his federal service in 1973 in the
19 Office of Secretary of Defense. I think you can see
20 he's extraordinarily well qualified for his current
21 task.

22 Dick, welcome.

23 (Applause.)

24 MR. CLARKE: Thank you, Tim, and thank you all

1 for coming.

2 I want to really thank Tim and Orson for putting
3 this together because we see this two-day workshop as
4 part of the national outreach effort that we are making
5 as we develop the national strategy that Tim mentioned,
6 the national strategy to secure cyberspace.

7 The President wants a national strategy, but he
8 doesn't want it to be written by a bunch of bureaucrats
9 who have worked in the Reagan Administration and the
10 Bush Administration and the Lincoln Administration.

11 He wants it written by and with the public, and
12 that's a unique challenge. How do we get the consumer,
13 how do we get the enterprise operator to think that this
14 is her problem or his problem to the extent where they
15 feel that they need to help us draft a national
16 strategy.

17 Today's meeting is part of a series of meetings
18 that we're having designed to get public input, and we
19 thank the FTC for setting up a mechanism where there
20 will be an opportunity for public input.

21 We're also having town meetings. We had the
22 first town meeting last week in Denver and next week in
23 Chicago and then Portland and then Atlanta, again to ask
24 people to think about the problem as part of our

1 awareness effort, but also to ask people to tell us what
2 they think on key issues before the strategy is
3 developed.

4 The other part of the openness and transparency
5 of the national strategy is that it will be online.
6 Sections of it will be written by the interest groups
7 themselves. The section on how we secure the vast
8 computing powers of American universities will be
9 written by American universities.

10 The section on how we secure the banking and
11 finance sector will be written by the banks themselves
12 working together and so on throughout all of the key
13 sectors of our economy.

14 The strategy will also be one that can be
15 quickly changed. It has to be capable of living in
16 Internet time and changing on Internet time, so that
17 when we see the threats change, so that when we see that
18 what we're doing isn't working, so that when we get new
19 ideas after it has first gone online, it can still
20 change and adapt. Our goal is to put the first strategy
21 online before the end of the summer.

22 The topic today deals with privacy and deals
23 with the consumer. Our strategy envisions five levels
24 and policy at five levels, beginning with the global

1 level, global policy. Orson Swindle has been working
2 with OECD as part of our international effort.

3 The fourth level counting down, the fourth
4 level, national level issues such as what's our research
5 agenda, what awareness program should we have, what
6 education program should we have.

7 The third level involves the work of the various
8 sectors of our economy like banking and finance, like
9 transportation, like electric power, what should they do
10 together.

11 The second level is what should be done at the
12 large enterprise, how do you secure a big company.

13 The first level is the topic we're dealing with
14 today, and that is what should be done to help the
15 average consumer, the home user, and the small
16 business?

17 This is a new thought. In the past, national
18 plans and activities focused on cyber security have not
19 focused on the average home user, and most of us,
20 whether we work in banking and finance or the government
21 or the press or academia, are home users, and there are
22 important questions, which we need to address as we put
23 this national strategy together.

24 Let me suggest some of them. I know many other

1 speakers here are going to raise them over the course of
2 the next two days. Particularly since I see so many
3 familiar faces in the audience, I know these questions
4 are going to be raised, but nonetheless, let me suggest
5 a few for you.

6 How can the home user without knowing it hurt
7 other people? Tim mentioned distributed denial of
8 service attacks, and we've seen that happen already.
9 This is not a theoretical possibility where the home
10 user, without knowing it, has their computer attacked.

11 Their computer is then -- a part of their
12 computer is then covertly taken over by an automated
13 program, and it sits waiting for instructions or it sits
14 waiting for a time, and then when that time comes, it
15 launches what's called a distributed denial of service
16 attack, firing messages out many times a second, and it
17 does it in concert with hundreds or thousands of other
18 computers, and those messages from all of those
19 computers are aimed at one site on the Internet.

20 The effect can be that that site closes down
21 under the volume, that the routers and the servers crash
22 under the wave.

23 Last July we had a similar experience, it was
24 called Code Red where servers, not home PCs, but servers

1 were infected. Tens of thousands and then 20s of
2 thousands of servers were infected by a virus that
3 became a worm, and on signal it was going to attack one
4 web site.

5 And as we became aware of tens of thousands, 20,
6 30, 40, a hundred thousand servers being infected, and
7 we could watch the number go up by the hour, we worked
8 in the government and in the private sector together as
9 a team to try to figure out what to do.

10 The first question was, whose web site was it
11 that was going to be attacked by this massive denial of
12 service attack, and when was it going to occur. About
13 four o'clock in the afternoon, I got the news, I was
14 going to say the good news, but I got the news whose web
15 site it was going to be. It was mine, that is to say,
16 it was White House.GOV. And when was the attack going
17 to occur? Four hours later.

18 We thought about that and said, Well, you know,
19 maybe the White House web site will just come down for
20 repairs this afternoon so we won't actually be knocked
21 off and be embarrassed. Then we thought a little bit
22 more. The White House web site wasn't the point.

23 The point was that a massive tsunami of that
24 scale coming down the Internet, going toward one site

1 would knock off routers and switches as it came down the
2 Internet, so it would damage much more than just our
3 ability to put up the daily press briefing on the White
4 House web site.

5 And so working together with the private sector,
6 with government agencies, quickly scrambling between
7 four o'clock in the afternoon when we figured it out and
8 eight o'clock in the evening when it was supposed to
9 occur, we developed a strategy, and that strategy was to
10 go to the Internet service providers, the big ones, and
11 say to them, Block traffic coming to us, not at the core
12 servers but at the edges of the Internet.

13 Well, you might imagine the reaction when you
14 pick up the phone and you call one of the large ISPs and
15 you say, Hi, I'm from the White House, I want you to
16 block all traffic to the White House. It took a little
17 bit of persuading, but by eight o'clock, all of the
18 major ISPs had not only agreed to do it, they had done
19 it, and they had blocked all traffic to that IP address
20 at the edge servers, and when eight o'clock came,
21 virtually nothing happened.

22 That tsunami did not occur, and that denial of
23 service attack was not successful, but that's one of the
24 big ones that you hear about. In point of fact, denial

1 of service attacks occur every day. There are hundreds
2 a month aimed at all sorts of different sites all over
3 the Internet and all over the world, and many of them
4 are happening because the home consumer hasn't been told
5 how to prevent his or her computer from becoming a
6 zombie. Many people don't even know when their computer
7 has become a zombie.

8 How else can the home consumer hurt other
9 people? If you work at home, as more and more people
10 do, or if you are forced to work out of a hotel room
11 when you're on the road, as more and more people are
12 regrettably forced to do -- we used to play tennis and
13 swim in the hotel pool, now we're online all the time --
14 you can hurt your company by doing that.

15 Sometimes you want to hurt your company when
16 you're doing that, but without intending to because your
17 home PC or your laptop that you take on the road can be
18 infected with a virus or a worm, and when you connect to
19 your office, sometimes you connect through what's called
20 a virtual private network that allows you to go in
21 securely behind your company's firewall.

22 Well, that's good, isn't it? It's a secure
23 connection. Yes, the connection is secure, but the PC
24 from which you're operating your laptop in the hotel

1 room, your desktop at home, may not be secure, and what
2 you have just done is established a secure net that
3 allows a virus or a worm or a back door to move
4 unchallenged through the firewall of your company and
5 into your company's network.

6 Because? Because you didn't have the latest
7 anti virus software. You didn't have the latest patch
8 on your operating system or application. You didn't
9 have a firewall through your home system, and your
10 company didn't require that you do, or if it required
11 it, it didn't have a way of verifying your software was
12 up to date.

13 It's a little more obvious how home users can
14 hurt themselves. They can hurt themselves by leaving
15 credit card information and other identity information
16 on their hard drives and then again not updating their
17 virus software, their operating system software, and if
18 they have a cable modem or if they have a DSL line, not
19 having a firewall.

20 I checked the other day a list of about ten
21 providers of DSLs, and I found only one of them that in
22 the course of saying, We offer you a DSL service,
23 mentioned that, Oh, by the way, you ought to get a firewall.

24 It's strange. It's a bit like offering someone

1 a car without an airbag or seat belt, and yet almost
2 every DSL provider with a few exceptions, almost every
3 cable modem provider with very few exceptions will
4 provide you that connectivity and say, Go for it,
5 without ever telling you that by having a constant
6 connection, by having a static IP address, you are
7 enormously increasing the chances that your computer
8 will be attacked, and if you don't have a firewall,
9 almost ensuring that your computer will be attacked.

10 So what should consumers do? Should they go out
11 every day to a web site and check for the latest virus
12 software, for the latest fix to their operating system,
13 for the latest fix to their firewall? It's a lot to
14 ask.

15 Now, some operating systems, some very common
16 operating systems in their latest version do offer
17 automatic updates. There are questions there about
18 whether or not you want someone doing automatic
19 updating. It's a question about how you know what
20 you're really downloading when you get that automatic
21 update.

22 Some virus software, in fact most of the major
23 providers now offer automatic updates, but should it be
24 so hard? Should we put that much burden on the

1 consumer? Should we ask them to worry about all of
2 these things, or is there a way in which we can
3 encourage Internet service providers, perhaps by
4 charging a premium, to offer secured service?

5 Frankly I think if most Americans were offered
6 the choice of connectivity for \$20 a month without
7 security features and \$22 a month with security, I think
8 almost everyone would go for the \$22 a month, and yet
9 that offer isn't there for most Americans. Most persons
10 cannot pay a little more and get their ISP to do that
11 work for them.

12 The ISPs can send you a firewall when they give
13 you a DSL connection or cable modem. They can scan the
14 software that you use to see if it's up to date, if you
15 allow them. They can automatically provide you updates
16 for common applications. They can make sure that your
17 anti-virus software is updated.

18 You really shouldn't have to worry about that
19 all yourself, but today you do. Most Americans are even
20 unaware that they need to do these things, so one of the
21 things that's already become very clear to us in
22 developing the national strategy is that we must give a
23 higher priority to national awareness.

24 I see many people in the audience who have

1 helped us already by creating the National Cyberspace
2 Security Alliance, companies, NGOs like SANS and others,
3 have helped us to put online a very helpful site called
4 StaySafeOnline.INFO. For those of you who haven't
5 seen it, I urge you to go there.

6 It's designed for the home user to tell them how
7 to secure their systems and how to get even more
8 detailed information if they want it. It's also
9 designed to help the parent who worries about letting
10 their child online at an early age.

11 I knew children were getting online at an early
12 age, but I didn't know how young until a week ago
13 Saturday when I saw a young girl, who's not yet three,
14 while I was talking to her parents, walked over, turned
15 on the computer, went, found the CD, put it in and got
16 up on the chair and started using the mouse and playing
17 with her CD, not yet three years old.

18 That's great, but it also means that she can do
19 it when her parents aren't around, and it also means
20 that having parents know about safety and parental
21 controls is becoming more and more important all the
22 time.

23 The other topic for this two day session -- in
24 addition to the issue of what the consumer needs to do,

1 the other topic is privacy, and many people have said to
2 me, How are you going to reconcile the requirements of
3 security on the Internet with the requirements of
4 privacy, and one of the questions that we put for
5 national discussion is to achieve IT security on
6 America's critical infrastructure, do we need in any way
7 to modify privacy rights.

8 I already know the answer to that, and it's no,
9 but I want that issue discussed, and I think it would be
10 a big mistake for us to develop an IT security strategy
11 for the country without spending a lot of time as
12 American citizens together talking about privacy rights
13 and our desire to maintain our privacy rights and to not
14 have them infringed as we increase security.

15 To me, privacy and security online are two sides
16 of the same coin. It's absolutely impossible to achieve
17 privacy without good IT security, and unfortunately,
18 what we're seeing all across the country is that privacy
19 information is being stolen because institutions are not
20 practicing good IT security.

21 I spent the day Friday at a major university in
22 the Midwest that told me of multiple incidents across
23 the country where Social Security numbers and other
24 information has been stolen at universities because

1 until now universities have thought that IT security was
2 anathema and somehow an infringement on academic
3 freedom. Well, not anymore.

4 Enormous computing power exists on university
5 campuses, and students need to ask and professors need
6 to ask of their university what is being done by that
7 university to protect their privacy rights.

8 One of the questions that has become popular in
9 the last six months is do we need a national identity
10 card, and I also know the answer to that. No. American
11 people, even in the wake of September 11, in all the
12 polling data, a large segment of the American people say
13 they don't want a national identity card, and I don't
14 think we need one, but we have to be careful in saying
15 no to a national security card that we don't say no to
16 user identity cards.

17 One of the ways that we can enhance security on
18 government systems is by having better identity cards
19 for government employees. The Pentagon has been
20 pioneering this with something called the Common Access
21 Card, that is an identity card with biometric
22 information on it that gets you into a defense
23 department building. It has a building pass, an
24 electronic building pass, and then also allows you to

1 log on to a computer.

2 Without that card, you can't log on to the
3 computer, and with that card, you can be assured that
4 the person's whose name is logged on is, in fact, the
5 person to whom the card was issued because it requires
6 biometric two source authentication.

7 It seems to be working. As with any large
8 program -- already over two and a half million have been
9 given the card. As with any large card, there are some
10 initial start up problems, but it does seem promising,
11 and we do need to ask whether or not security in
12 general, including privacy, at government institutions
13 could be enhanced by taking that kind of two
14 authentication smart card and requiring it as a way of
15 logging on to government systems, if you're a government
16 employee, either at work or at if you're telecommuting.

17 Security also raises the issue of anonymity. So
18 much of the security violations that have occurred on
19 the Internet have occurred by people who are anonymous
20 or who have spoofed their identity or who have stolen
21 their identity, and it does seem to me that we need --
22 while we embrace privacy rights, we need to ask if
23 there's a distinction between privacy and anonymity and
24 whether everywhere on the Internet is a place where you

1 should go anonymously or whether there are large
2 sections of the Internet where we need to prevent
3 anonymity.

4 Certainly there are some places where it doesn't
5 matter, but there are lots of places on the Internet
6 where anonymity is a great risk to security and to
7 privacy rights. I'm anonymous when I go to my county
8 library and wander through the book stacks, and that's
9 fine, but I shouldn't be anonymous if I go to the county
10 hospital and wander through the medical records. That's
11 not fine.

12 We need to make that distinction, and we need to
13 find ways of ensuring that when you are on a web site or
14 part of a network that has sensitive information and
15 privacy information, that you are not anonymous or that
16 you are not spoofing your identity.

17 There is another way in which security can
18 affect all of us, and it's when we do business with a
19 company or an institution that does not maintain
20 security. How do we know that when we provide our
21 information to a company or an institution, that it is
22 living up to some set of good practices for IT
23 security?

24 Typically we don't. If we do commerce online,

1 we may be able to see that the web site is using some
2 sort of encryption. We always look for that little lock
3 on the bottom of the web site before we put our credit
4 card information down.

5 Of course, I'm told it's rather easy to have a
6 little lock on the bottom of your web site whether or
7 not it's a secure site, and sometimes we look for the
8 name of a particular IT security company that is
9 guaranteeing the security of the transaction, and with
10 that we feel secure, and the transaction is secure, but
11 after the data goes into the database, that may not be
12 secure.

13 The information that you have seen on the web
14 site says that your session, your linkage to the company
15 is secure, but it doesn't tell you anything about what
16 that company's IT security practices are. Online
17 banking is a great thing, and you can tell frequently if
18 the web site is secure, but you are, for the most part,
19 unable to determine whether the bank has good security
20 practices.

21 There are no disclosure requirements. There are
22 no disclosure requirements about whether or not the bank
23 or other institution with which you are dealing with
24 online has been hacked. How often has it been hacked?

1 How badly has it been hacked? There are no disclosure
2 requirements about what its IT security practices are.
3 Who is the chief IT security officer of the company?
4 How much money is being spent as a percentage of revenue
5 or as a percentage of the IT budget on IT security?

6 When was the last time the organization, the
7 company had an outside vulnerability assessment? Were
8 the findings of that vulnerability assessment
9 rectified? These are things that you might want to
10 know.

11 When we dealt with institutions online prior to
12 the Y2K roll over, we were able to find out whether or
13 not the institution we were dealing with was Y2K
14 compliant, and most of us, in our monthly bills, got
15 long statements in small type face telling us something
16 about Y2K compliance from our credit union or whatever
17 institution it was we were dealing with, but you don't
18 get that today with your monthly bill or your stock
19 information if you happen to be an investor.

20 You are largely left in the dark as an investor
21 or as a consumer about the security practices of the
22 organizations with which you deal.

23 We all know that IT security is complex, but
24 there must be some simple statement that can be made

1 about compliance with some set of best practices. I
2 don't think the government should write those best
3 practices. I think industry groups together with
4 consumer groups should get together and establish some
5 notion of what best practices are for certain kinds of
6 companies.

7 But I do think somebody ought to provide some
8 list, some criteria for evaluating, if I'm going to do
9 business with a company, whether or not that company is,
10 in fact, secure.

11 These are all issues that we intend to address
12 in the national strategy. They're issues I hope you
13 address today and tomorrow and on an ongoing basis as we
14 develop the strategy, as we get it online and as we
15 continue to modify it.

16 We look forward to these two days. We look
17 forward to your input because it's vitally important to
18 us as a country that the IT revolution continue, that we
19 go into the next stage of that IT revolution, and that
20 we realize all the economic and social benefits that
21 will come when we move to the next step up the ladder of
22 IT deployment across the country, but as John Chambers
23 said in December, CEO of CISCO, we will not get to that
24 next step on the ladder of IT deployment unless we can

1 achieve IT security.

2 Thank you very much.

3 (Applause.)

4 MR. EICHORN: We do have a few minutes for
5 questions. If anyone has questions, you're welcome to
6 come up to the mike.

7 MR. ABRAMS: My name is Marty Abrams. Do you
8 have any thoughts about whether user IDs should be used
9 on home computers to assure better authorization and
10 authentication when dealing with sites?

11 MR. CLARKE: I think if you're dealing with a
12 site online where you want to have high level security,
13 not just on your end, but you want to know that the
14 organization when it deals with other people are also
15 secure. You know when you log on, but you're you, and
16 therefore you think, Why do I need to have some sort of
17 smart card to prove it.

18 It's not because you would abuse the system.
19 It's because the next person that logs on and says it is
20 a customer might abuse the system, so I would feel safer
21 personally if I were doing business with a company
22 online and it did ask me to use some sort of smart card
23 because then I would know that no one else is going to
24 be able to log in without having their identity in some way

1 verified.

2 I think that increases the chances that the
3 overall system, the overall network that you're
4 connected to, won't be compromised, and since you're
5 probably providing that network with privacy
6 information, with financial information, you want it
7 secure all the time, even after your session is over.

8 MR. CLARKE: Hi. Drew Clark with National
9 Journal's Tech Daily. When you talk with the tension
10 between anonymity and security, are you saying something
11 beyond the fact that individual businesses should be
12 permitted to require smart cards and other type of
13 things?

14 In other words, are you saying that there ought
15 to be some societal set parameters for when people can
16 be anonymous online and when people cannot be anonymous
17 online?

18 MR. CLARKE: No, what I'm saying is that I think
19 there are large sections of cyberspace where important
20 information is transacted. It doesn't have to be
21 consumer information. Sometimes it's consumer
22 information. Sometimes it's merely business to business
23 activity. Sometimes it's the management of the electric
24 power grid. Sometimes it's the management of a major

1 rail system.

2 For all of the critical infrastructure functions
3 and for most of the e-commerce sections, I think
4 anonymity is a security risk to the individual. There
5 are clearly large sections of the Internet where it
6 doesn't matter.

7 Before coming over here, I thought I would try
8 to find some jokes about consumer protection, and so I
9 went online and found five sites with jokes about
10 consumer protection. I think I ought to be able to do
11 that anonymously.

12 MR. FOX: Jeff Fox, Consumer Reports. You
13 mentioned before that we're going to be developing a
14 national strategy, a national policy for information
15 security. You mentioned that certain industries will
16 develop a strategy with input from the industry.

17 Are we going to be developing a strategy for
18 consumer's home computers, and will consumers be
19 developing that strategy, and what kind of input will
20 you get from consumers?

21 MR. CLARKE: Level one of the strategy is about
22 the home user, and we are looking for ways to find
23 groups, consumer groups to help us draft that strategy,
24 and if you can give us ideas about that, we would

1 welcome it.

2 MR. LANE: Hi. I'm Terry Lane with Washington
3 Internet Daily. The cyber security strategy, will there
4 be any provisions to compel industry to adopt certain
5 guidelines or regulations? How would that work as part
6 of enforcement?

7 MR. CLARKE: I think in general having the
8 government compel industry to do certain things with
9 regard to cyberspace security is probably a bad idea. I
10 say in general because the Congress has already passed
11 the Gramm-Leach-Bliley Act on banking modernization
12 which does include some cyber security regulation, and
13 it's also passed HIPAA legislation on health care which
14 also applies some regulation with regard to cyber
15 security.

16 I think in general regulation is a pretty -- in
17 the area of cyberspace security in general is likely to
18 be pretty ham-handed. By the time that we were able to
19 write, publish, get comment on and go into effect
20 cyberspace security regulations, they would likely be
21 outdated since the technology and the networks and the
22 system so rapidly evolve.

23 So what we're trying to do instead is to
24 stimulate the marketplace and to encourage codes of best

1 practices, sets of standards that are developed by the
2 vendors and by consumers, by the critical
3 infrastructures that use the technology and then to have
4 those standards and those best practices clearly and
5 publicly articulated.

6 The banking and finance community is on its own
7 now developing a set of cyber security standards one by
8 one. They started off with wireless security, which I
9 always thought was an oxymoron, but in any event they
10 are developing cyber security standards, and people will
11 be able to see them and know whether or not their
12 institutions are participating in these voluntary
13 standards.

14 I think that probably given the technology
15 aspect and the speed aspect is the best way of doing it,
16 not compulsory government regulation.

17 MR. EICHORN: Dick, this will be the last
18 question.

19 MS. FRAKER: Hi. I'm Mary Fraker from Powell
20 Tate. I was wondering what kind of monitoring
21 capability you have that enabled you to anticipate this
22 enormous attack on White House.GOV, how you knew all
23 these things were flowing out and waiting.

24 MR. CLARKE: We don't have a monitoring

1 capability, but the Internet service providers do. They
2 monitor their own network, and what they were able to
3 see was a rather large and unprecedented spike in
4 network traffic, which led them to try to figure out
5 what it was.

6 And then we received from NGOs like SANS, Alan
7 Paller is here from SANS, from other organizations like
8 CERT at Carnegie Mellon, we were told by these non
9 governmental institutions that something was going on,
10 and they then began to figure out what it was. Rich
11 Pethia played a company role, back here in row five,
12 over that weekend in figuring out what it was and
13 telling the government what it was.

14 There is no Internet command post. The Internet
15 is dispersed. There's no place in the government that
16 monitors the Internet, so we rely heavily upon the
17 cooperation of industry and NGOs like CERT and SANS to
18 tell us when there's an anomaly, and then we have to
19 work with them.

20 The government can't solve these things by
21 themselves. When we talk about public private
22 partnership, we talk about it so much that sometimes
23 people get sick of hearing me say it, but the reason we
24 talk about it so much is that this is a problem that

1 does risk our national infrastructure. It does risk our
2 national economy. It does risk our national defense,
3 depending upon who the actor is and what they're doing.

4 The government can't do it itself, the
5 government can't defend this country's cyberspace itself.
6 The FBI, the Army, the Navy, put them all together, they
7 can't do it. Cyberspace has to be defended in
8 cooperation with the government because we have some
9 information and assistance and some capabilities that we
10 can provide, but whether it's your home cyberspace or
11 the cyberspace of the electric power grid or the
12 cyberspace of the railroad industry, you really have to
13 do it yourself.

14 MR. EICHORN: Thank you, Dick.

15 (Applause.)

16

17

18

19

20

21

22

23

24

1

2

3

4

5

6

7

8

9 "PANEL 1: Current State of Consumer Information Security"

10 MARK EICHORN, MODERATOR, FTC

11 MARY J. CULNAN, PH.D., Slade Professor of

12 Management and Information, Bentley College

13 LAWRENCE DIETZ, Director of Market Intelligence

14 Communications, Symantec Corp.

15 JEFF FOX, Senior Projects Editor, Consumer

16 Reports

17 BRUCE HEIMAN, Executive Director, Americans for

18 Computer Privacy

19 ROB LEATHERN, Analyst, Jupiter MediaMetrix

20 RICHARD PETHIA, Director, CERT Centers

21 MR. EICHORN: Panel 1 panelists, do you want to

22 come on up?

23 Hi. Hello again. I'm Mark Eichorn. I didn't

24 introduce myself earlier. I wanted to introduce Jessica

1 Rich and Ellen Finn and Laura Berger up here in front,
2 we are together the team that's been responsible for
3 putting this together, and Maureen Cooney, who will be
4 doing the international panel.

5 Just ground rules for today for the panels,
6 every one of our panelists has an illustrious history,
7 and those are provided in your packets in the bios.
8 We'll be making very brief introductions this afternoon
9 and this morning.

10 Also for the panelists, I would like to remind
11 all the panelists to stick more or less to the time
12 limits that we've discussed earlier just so that we can
13 keep on schedule.

14 Our first panel is the Current State of Consumer
15 Information Security, and we're going to be talking
16 about issues such as what the risks are and how the
17 risks are changing and what the harms are and the impact
18 on consumers, so if any of you have remarks on Dick
19 Clarke's views, we may get to that as well.

20 At some point during this panel, we're going to
21 take a break and then reconvene with the same panel, but
22 we will basically go for the morning here.

23 Rich Pethia, I would like to start with you.

24 Rich is the manager of the Network Systems Survivability

1 Program at the Software Engineering Institute, the
2 director of CERT, and he's also active in the Internet
3 Security Alliance.

4 Rich?

5 MR. PETHIA: Yes, what I wanted to do is just
6 highlight some of the things that Dick Clarke mentioned,
7 the first one being is that this is a problem that is
8 here today. It's not one that we might see sometime in
9 the future. It's not one that we have five years to get
10 ready for.

11 We are one of about 160 different security
12 incident response teams scattered around the planet, and
13 every day we receive reports of intrusions in the
14 systems. We receive reports of denial of service
15 attacks. We receive reports of systems being
16 compromised in one way or another, and in fact we get a
17 lot of reports.

18 Last year we had over 52,000 separate incidents
19 reported to us. Things like Code Red and the Nimda worm
20 each count as one in that list, and so while there are
21 some of these things that make the press occasionally as
22 big news items, the real fact is these things happen
23 every day, and the problem is growing.

24 Last year, as I said, we had 52,000 incidents

1 reported. The year before that it was about 20,000.
2 Right now with the first quarter numbers in it looks
3 like we're on track for almost a hundred thousand
4 incidents reported this year.

5 The problem in terms of number of reports being
6 generated is doubling every year, and that's just that
7 data that we see at our center. That does not count the
8 data that's being pulled at those 160 other
9 organizations or in organizations like SANS that also
10 receives reports from the outside community.

11 Another key point I think is that this is not a
12 static problem. It's not like there are 16 things out
13 there that we have to fix, and once we fix them the problem
14 goes away. This problem changes every day. There are new threats that
15 occur on a regular basis. The intruders, the
16 bad guys, understand the technology. They learn more about
17 it every day. They're getting better at finding flaws in the
18 technology.

19 They share this information with one another.
20 Especially over the last five years, since 1997, we've
21 seen the widespread use of automated tools that are now
22 available widely on the Internet. These tools have now
23 literally brought us to the point where there's a point
24 and click attack culture where people with very little

1 technical sophistication can successfully attack other
2 machines connected with the Internet because the attack
3 technology itself has evolved to the point where it's a
4 very easy thing to do.

5 Another point is that the technology that we all
6 rely on, the laptops, the PCs that we have in our homes,
7 the servers that we have in our corporations, all of the
8 products that are out there in some way or another have
9 some significant number of security flaws.

10 Again in 2000, in the year 2000, we had about
11 2,500 security vulnerabilities that were reported to
12 us. This year -- and by vulnerability I mean a flaw in
13 the software that allows an intruder to take advantage
14 of a flaw and somehow get better access or get access to
15 the machine. This year at the current reporting rate,
16 we're on track for almost 5,000 new vulnerabilities
17 being reported.

18 So the attack technology continues to change.
19 The technology that we're dependent on continues to be
20 faulty in one way or another, and so whatever solutions
21 you have in place today, you can be virtually assured
22 that you're going to have to do something different
23 tomorrow because the picture's going to change yet
24 again.

1 So it's a problem that's here today. It's
2 growing. It's changing. It is becoming more
3 significant, and for the little bit of data that we all
4 have on impact, and there are very few comprehensive
5 surveys available, but the Computer Security Institute
6 in collaboration with the FBI does an annual survey on
7 the impact of some of these problems, and we see from
8 that data on a year by year basis, as limited as it is,
9 there are significant losses being incurred at financial
10 organizations, and you can be assured that in one way or
11 another as consumers those losses will be passed on to
12 you.

13 So I think there's a lot of work to do. It's a
14 problem that as I said we don't have time to get ready
15 for. We have to start dealing with it now. I think
16 there are lots of avenues available to us to attack the
17 problem from improved technology, to more awareness, to
18 more advocacy and activity on the part of consumer
19 groups.

20 I think one of the things that's really missing
21 right now in the world is a set of advocates for
22 consumers who can help get this issue on the table,
23 increase awareness and begin to bring pressure to bear
24 against the technology producers and suppliers to

1 produce a better product that we all depend on.

2 And hopefully the next discussions over the next
3 couple days will highlight more of these issues.

4 MR. EICHORN: Thank you, Rich. Rob Leathern,
5 Rob is an analyst at Jupiter MediaMetrix covering
6 online payments. His research focuses on using the
7 Internet to enable and streamline financial transactions
8 for consumers and businesses.

9 Rob?

10 MR. LEATHERN: Thanks. As some of you may know,
11 Jupiter MediaMetrix is an online market research and
12 analysis company. MediaMetrix is our audience
13 measurement. We have a panel of over a hundred thousand
14 U.S. users, and we can monitor what sites they visit and
15 other aspects of their online behavior patterns.

16 Jupiter Research, which is the group I work for,
17 does research into what consumer behavior and --
18 business behavior when they're dealing with consumers
19 goes in to. I myself have been responsible for helping
20 inform businesses how they should encourage consumers to
21 interact with them through web based and wireless
22 interfaces, specifically looking at transactional based
23 businesses such as online retail and online financial
24 services.

1 And I really agree with Mr. Clarke this morning
2 that privacy and security really are two sides of the
3 same coin. We find that overcoming security and privacy
4 fears relating to credit card and personal information
5 is the biggest thing holding back people from making
6 online purchases.

7 In fact, of people who browse and look for
8 product information online, that is people who have not
9 yet made an online purchase, 51 percent say that better
10 security for their credit card or personal information
11 is what is required before they will consider making a
12 purchase online.

13 We also find that there's kind of an incremental
14 adoption pattern that consumers undergo. They will sign
15 up for Internet access. They will be checking and
16 receiving emails. They will then move on to things like
17 online purchases, eventually moving over to conducting
18 online banking and bill payment.

19 In fact, online bill payment is one of the
20 greatest growing applications we've seen over the past
21 two years, two to three years. So really that is
22 something that is really growing and is threatened by
23 some of these security concerns we see out there.

24 The trade-off between convenience and security

1 is one that continues to challenge businesses. There's
2 also evidence that it's really been way too convenient
3 for consumers up to now.

4 We did a survey in August last year where we
5 asked consumers if they would be willing to undergo, to
6 undertake certain additional activities to strengthen
7 the security of credit card transactions online. What
8 was interesting about the survey is we asked pretty much
9 the same question for consumers about their online
10 transaction experiences as we did about their offline
11 transaction experiences.

12 24 percent of people say that they saw no need
13 to increase credit card security offline, but only 14
14 percent of consumers saw no need to increase security
15 online. It appeared that many consumers were willing to
16 undertake additional activities in order to strengthen
17 the security of their credit card information.

18 For example, 49 percent of people say they would
19 be willing to type in an additional pin or password
20 created or provided to them by the credit card company.
21 As many of you may know, VISA is working on an
22 initiative called Verified by VISA. You may have seen
23 the T.V. commercials with Emmitt Smith.

24 What it basically is is when you conduct a

1 transaction, credit card transaction online, you get
2 taken then to your bank card issuer site where you would
3 be verified or you would be authenticated as the person
4 you purport to be.

5 That's just an example of some additional
6 security measures that make it a little more
7 inconvenient for consumers to conduct transactions
8 online, but frankly I think it's been a little too easy
9 for consumers to date, and clearly the payoffs for
10 businesses moving consumers online is great.

11 If you look at, for example, the financial
12 services area in banking, processing a transaction at a
13 branch costs perhaps five times as much as processing an
14 online transaction. Communication, sending an email can
15 cost a fraction of a penny versus 50 to 80 cents perhaps
16 for sending an offline communication.

17 Recently we have see seen incidents, for
18 example, Bank of America had a problem a few months ago
19 where someone was sending out emails purporting to be
20 Bank of America to customers. These are the types of
21 things that can increase the costs of sending email
22 communications, and perhaps maybe the cost of email
23 communications should be higher because it's just way
24 too easy to send emails to the list -- go visit Millions

1 of Addresses.COM and you will find that you can quite
2 easily buy a CD Rom of 5 million email addresses and
3 email people at will.

4 We believe at Jupiter that several trends are
5 converging to increase possible security risks. Today
6 of people we surveyed, over 60 percent of people would
7 give their email address in exchange for a hundred
8 dollars sweepstakes entry. 41 percent of people would
9 type in a user name and password at a site that they
10 hadn't done business with before in exchange for the
11 self same sweepstakes entry.

12 If you add to that some brand new data that we
13 actually haven't published yet but just came out a few
14 weeks ago, that 53 percent of users use the same user
15 name and password at all or most of the sites they
16 visit, you can put these two numbers together and find
17 out that if you have a really interesting sweepstakes
18 offer, we all know it's pretty easy to brand yourself
19 online, at least to look legitimate with graphics and
20 other things, you can see that this is a big problem.

21 Sites quite easily gather -- appearing to be
22 legitimate gather user names and passwords and then use
23 those to compromise people's accounts, and we're not
24 just talking anymore about someone going and buying a

1 \$12 CD at Amazon.com. We are talking about people that
2 increasingly have and are managing financial
3 relationships, assets at brokerage accounts and banking
4 institutions that can now be compromised by some of these
5 aberrant password behaviors.

6 Consumer perceptions of the safety of their
7 information are very apt to be influenced by widely
8 publicized but infrequent events. You may have read the
9 news a few days ago, Ford Credit I think they had, what
10 was it, 13,000 credit reports compromised. Similar to
11 some of the risk perceptions you get around driving your
12 motor vehicle versus taking the airlines, obviously it
13 appears when there's an incident in an airline context,
14 it's much larger.

15 Obviously people have a much bigger fear of it,
16 so you have this misperception of risk for one thing, so
17 people need to be informed about they should be taking
18 ongoing precautions, and the other problem you really
19 see is that all companies are negatively affected by a
20 lack of confidence in the online medium.

21 So even the practices of those companies who are
22 doing a great job are negatively affected by those
23 companies that are doing a poor job. There's a real
24 need to better educate consumers, encourage and monitor

1 security best practices, and reward companies who are
2 doing a good job of the above.

3 Unfortunately, one of the biggest, unresolved
4 issues is who is going to pay for all of this. I've
5 spoken in the last couple days to one of the top three
6 banks in the United States, and they are totally on
7 board with the idea of it, but unless really compelled
8 to do so, they're not going to be extremely proactive
9 and spend a lot of additional money in order to make
10 this happen.

11 So I think that's the question I would leave off
12 my prepared comments with is someone needs to figure out
13 how we proactively encourage companies to spend money to
14 help educate the consumer.

15 Thanks.

16 MR. EICHORN: Thank you.

17 Bruce Heiman, Bruce is the executive director of
18 Americans for Computer Privacy and a partner at Preston
19 Gates. He concentrates his law practice in the areas of
20 IT, trade and transportation.

21 Bruce?

22 MR. HEIMAN: Thanks. Americans for Computer
23 Privacy is a broad based coalition of more than a
24 hundred companies, 40 trade associations and some 7,000

1 individuals. We really led the fight during the '90s to liberalize
2 export controls on American encryption
3 products. For the last two years, we've been working
4 hard to ensure that our nation's critical information infrastructure is
5 protected in the right way.

6 This morning I want to focus on consumer
7 information security and make three points. First, I
8 want to urge everyone to "gas" up in cyberspace. I want
9 to make sure that everybody guards against strangers
10 online.

11 Second, I want to offer a handful, really five
12 specific, practical tools that consumers can use to
13 protect themselves, and third I want to recommend three
14 things that the government can and should do and two
15 things that the government definitely should not do to
16 help the consumer.

17 So why should we worry? Why should we "gas" up in
18 cyberspace? When they asked Willy Sutton why he robbed
19 banks, he said, Well, that's where the money is, so it
20 shouldn't be surprising that in the information age,
21 criminals are targeting information.

22 One important difference is Willy Sutton let
23 people bring their money to the bank to a centralized
24 location, but technology now allows for distributed

1 victims. With computers it's now possible and
2 profitable for criminals to reach out and touch people
3 where they are.

4 I would hope that the public understands that
5 computer crime is real crime. It's not funny. It's not
6 a joke. It's not cute, and anyway you look at it, as
7 you've heard, the problem is clearly getting worse.

8 What's interesting is it's not only getting
9 worse in absolute numbers but it seems to be getting
10 worse relatively as well, that is, if you take the
11 number of incidents and compare it to sort of any
12 measure of online activity, whether it's number of
13 computer users, number of computers, hosts, clients, in
14 relative terms the problem is also getting worse.

15 So, what can consumers do about it? Plenty.
16 The tools exist, and they are available for individuals
17 and companies to protect themselves if they take the
18 threat seriously. I want to emphasize this. Security
19 can only be improved if users take advantage of the
20 security tools that are available to them.

21 It's not rocket science. It's not even computer
22 science. It's common sense so with that in mind, let me
23 offer a handful of suggestions, five specifics that have
24 been suggested by the Business Software Alliance and

1 others: Use strong passwords; change them frequently;
2 use anti-virus software; install a home firewall;
3 update your security features regularly; and encrypt
4 your stored data.

5 Now, if everybody did this, we would be an
6 incredible ways down the road to good security
7 nationwide.

8 Finally, I want to talk about what the
9 government itself should and should not do to help
10 secure consumer information because there are definitely
11 right ways and wrong ways for the government to get
12 involved.

13 Three things the government should do: First,
14 educate. Workshops like this are excellent. So too is
15 the Administration's recent National Cyber Security
16 Alliance. The government can play an important role in
17 educating all of us about the importance of essentially
18 practicing good security hygiene.

19 The government also can remind the public that
20 cyber security is an ongoing responsibility. There is
21 no silver bullet. There is no one time fix.

22 A second thing government can do is enforce the
23 cyberspace laws. At this point the laws are basically
24 on the books making computer hacking, theft and

1 destruction crimes. Now comes the hard part,
2 investigating, prosecuting and punishing those who
3 commit such crimes.

4 The government needs to make it a priority to
5 devote adequate resources to the job and train law
6 enforcement personnel.

7 The third thing government can do is remove
8 barriers to information sharing about cyber problems and
9 solutions. Right now companies are reluctant to share
10 information because they fear it will be disclosed and
11 used against them.

12 Pending legislation in the House and the Senate
13 fixes this problem by offering limited protection for
14 shared information.

15 Now, there are two things that government should
16 definitely not do. First, do not mandate the use
17 of particular security technologies, processes or
18 products. The government should not be in the business
19 of promulgating technology specific standards. Doing so
20 will make the cyber security problem worse by stifling
21 innovation, freezing development and artificially
22 channeling R&D.

23 Cyber security is best accomplished through
24 private sector solutions that are market driven and

1 industry led.

2 As you heard today, it's essential to remember
3 that the private sector designed and deployed today's
4 computer networks and products. The private sector owns
5 and operates them, and they have really the knowledge
6 and expertise to best develop cyber security solutions.

7 The other thing government should not do is
8 weaken individual security. You might ask, Well, why
9 would they do that or how could they do it? Well, first
10 they shouldn't weaken the ability of individuals to
11 protect themselves against cyber crime by limiting
12 the ability of American industry to develop best
13 products and services.

14 How could this happen? One good example were
15 the efforts during the '90s to try to require that
16 American companies install back doors into their
17 encryption products or to require that an extra set of
18 keys be given to the government.

19 Another example would be requiring ISPs to build
20 their systems in such a way that permitted easy,
21 immediate access to law enforcement. On the telecom
22 side, this was the CALEA debate. This came up with respect to ISPs as
23 part of the Council of Europe cyber crime convention, which
24 unfortunately was not adopted.

1 Government should also not reduce our security
2 under the guise of helping law enforcement, and a good
3 example of this is a requirement that ISPs keep all
4 communications for 90 days. That would be good, but
5 you're also creating -- on the one hand you can go in
6 and try to investigate. On the other hand, you're now
7 creating a new repository of data that itself becomes an
8 attractive target.

9 Also, as originally proposed, Fed.Net was a
10 government-wide Internet -- it was a government proposal
11 to have an Internet surveillance system. That has now
12 been scaled back appropriately towards more of a
13 management tool, a network administration tool for
14 government networks itself.

15 So to review, we must guard against strangers
16 online. We should take five actions to protect
17 ourselves, and government should take three actions to
18 help, and definitely not take two other actions.

19 Thank you.

20 MR. EICHORN: Thank you, Bruce. Mary Culnan,
21 Mary is the Slade Professor of Management Information
22 Technology at Bentley College in Waltham, Massachusetts,
23 author of the Georgetown Internet Privacy Policy Survey,
24 and coauthor of the Culnan-Milne survey.

1 Mary?

2 MS. CULNAN: Thank you very much, and I want to
3 thank the FTC for organizing and hosting this workshop.
4 It's really needed as we heard from Dick Clarke, and I
5 hope that this will be the beginning of efforts that
6 will do for security, particularly consumer and small
7 business security, what their privacy workshops have
8 done for privacy in terms of promoting the discussion.

9 I'm going to try and put a human face on
10 security and follow up on some of the things that Dick
11 Clarke talked about. Actually he gave my remarks minus
12 one example, but I think one of the issues that I think
13 is very important is that the vulnerabilities extend far
14 beyond what people make experience in terms of loss of
15 their own data or alteration of their own data on their
16 home computer, that once you get broadband access and
17 you're connected to the Internet, you're really
18 connected to the world.

19 And therefore consumers that don't protect their
20 home systems represent a threat to critical
21 infrastructures, to our national security because that
22 also includes their economic well-being, and as we heard
23 their home computers can be used to launch denial of
24 service attacks.

1 Just this year the National Academy of Sciences
2 issued a report on cyber security called "Pay Now or Pay
3 Later," and in it, it cites the use of unexpected home
4 computers to launch some of these attacks, and there's a
5 real cost of these as we heard.

6 The CSI FBI survey reported that 10 percent of
7 their respondents, granted that was a very small number,
8 but they had experienced denial of service attacks, and
9 the average cost to clean up one of these was \$122,000,
10 which if you add all of these up turns into real money.

11 So is this a real problem? And this is where I
12 want to get into a couple examples. I had a student in
13 a class last fall who came into class one night and
14 reported she had a DSL line with no firewall, and she
15 got hacked, and whoever attacked her came in and they
16 hi-jacked her AOL account and used it to launch a SPAM
17 attack.

18 The only reason she had any idea this had
19 happened is because AOL had shut down her account
20 temporarily because she had sent out too much email, and
21 she was really in a panic. She didn't have any idea of
22 what to do now, was there still stuff on her computer
23 that was going to be a problem, had her system been
24 compromised? And so this is only one example, but she's

1 clearly not the only one.

2 My own experience, I moved into the broadband
3 early this year. I got a new computer that has
4 Microsoft XP, and I installed a cable modem and
5 installed a firewall, and within five minutes of
6 installing the firewall started getting scanned because
7 the firewall software would give you a pop up alert.

8 And over the past two or three days which is
9 where I've been logging in, I've been getting 20 to 30
10 of these scans a day, and these are scans where
11 somebody's actually looking at your computer to come
12 in.

13 They're not legitimate interactions with known
14 firms on the Internet, so this suggests that in fact
15 this is a real problem, and it's going to get bigger,
16 and while you have a firewall and you have good
17 anti-virus software, you're not going to stop a really
18 determined attacker who wants to do serious damage.

19 It wants to cut down on these sort of nuisance
20 attacks. Just like putting a lock on your front door or
21 a club on your car is going to send a burglar to look
22 some place that's not secure.

23 So what should we do? Obviously there's a need
24 for a lot of consumer education. I teach privacy and a

1 little bit of security at Bentley, and even with
2 students who have been exposed to technology and should
3 be relatively sophisticated, you don't get a good
4 proportion of those that have broadband access having
5 the appropriate software in place, and so there needs to
6 be a lot of work on this.

7 I know Jeff Fox is going to talk about the
8 Consumer Reports article that just came out. I think
9 this is a terrific example of what needs to be done, not
10 only talking about the problem but they rate software
11 products and give people some tools that they can go out
12 and either purchase or download immediately to put some
13 protections in play.

14 And I also want to second Dick Clarke's call
15 that the vendors and the ISPs should step up to the
16 plate. I think this is irresponsible of them not to do
17 so. Microsoft's XP comes with a basic firewall, which
18 is an excellent first step because you really don't have
19 to do anything except you do.

20 They don't turn it on or and they don't really
21 provide you any kind of heads up when you install the
22 software or start running it that in fact you should
23 turn on the firewall. I found out about the firewall
24 when I went to the computer store and went to buy a firewall

1 and asked if it would be compatible with XP and was
2 told, You don't need a firewall, you already have one,
3 so I went out and bought a box and was in business.

4 When you turn it on, it doesn't seem to affect
5 your system at all so I don't see any reason why it
6 shouldn't be on, and hopefully we'll hear from them.

7 I think the broadband vendors or the ISPs should
8 also bundle security software with their services or
9 make it easy for people to download it and have them
10 turn it on as part of the installation process.

11 When I installed my -- got my cable modem
12 installed, it was a third-party contractor who did the
13 installation, and he didn't know anything about firewalls
14 or should I have one them or whatever and so I found that kind of
15 disappointing.

16 Finally, I think government can't solve this
17 problem but it can certainly help. Chairman Muris, the
18 FTC, and lots of other people in the government have the
19 bully pulpit, and when they go and speak to the public,
20 they can continue to encourage people to do better.

21 I also think that good security should be a
22 requirement for any broadband funding expansion program,
23 so if there's money given to telecom companies to go
24 out and expand the reach of broadband to consumers, then

1 that should carry a requirement that they also provide
2 appropriate security when they install these services.

3 MR. EICHORN: Jeff Fox is a senior projects
4 editor for Consumer Reports. He's been covering
5 technology, cyberspace and privacy for a dozen years now
6 or so.

7 Jeff?

8 MR. FOX: Thanks, Mark. First of all, I would
9 like to express my appreciation to the FTC for having
10 this workshop and for timing it about ten days after the
11 article on which I spent months working came out. Had
12 it been before the article came out, it might be a
13 little more difficult to speak about.

14 Also I want to mention to Rich that at least one
15 major consumer organization is now on the case, and I
16 would like to thank CERT for the help that they provided
17 us in the investigation, and I just completed this
18 lengthy investigation on essentially the subject of this
19 workshop.

20 The information that was turned up is too much
21 information for the few minutes that I have here, so I
22 recommend to people to look at the June issue of
23 Consumer Reports. If you need a copy or press kit, I
24 can provide that for you. Thank you.

1 Also after these remarks, I'll be delivering a
2 written report with a little more detail and analysis to
3 the Commissioners, and if they want to put some of that
4 -- including some graph charts and data, and if they
5 want to put that up on their web site, they're free to
6 do that.

7 I guess the center piece of the report was a
8 survey that we did of about 8,000 of our online
9 subscribers, and I'm required by our survey researchers
10 to give a little caveat that these were online
11 subscribers and not completely representative of the
12 American public, although they characterized themselves
13 as intermediate and advanced users, so we kind of expect
14 that their experience would possibly be better than --
15 or they would be as well or better protected than the
16 average person.

17 The subjects that we have focused on in the
18 article were hackers and unprotected broadband home
19 users and malware viruses and Trojans and the like.

20 The problem of unprotected broadband users, our
21 survey showed about 35 percent of the figures that we
22 surveyed did not have a firewall installed. This is
23 the one piece of data that we've actually been able to
24 back up with data about the general public. We've done

1 a subsequent survey that's not yet published that shows
2 that this number is in the ball park, so that's one
3 number that I mentioned today that can be generalized to
4 the general public.

5 If you apply that to the number of online
6 broadband users, you get at least several million users
7 out there now that don't have a firewall who have high
8 speed connections, and I would say that this is now -- I
9 view this now as a cyberspace equivalent of
10 Afghanistan. This is a breeding ground for criminals and
11 terrorists. It's really just a time bomb waiting for
12 the right person to set it off or people to set it off.

13 We didn't get a lot of data in our survey about
14 hacking. We did get a small number of people that said
15 they had been hacked, but the data was kind of skimpy.
16 We got much more information about people's experiences
17 with viruses and worms, and I'll just run through them
18 quickly, but the data will be available in that report.

19 Of the people that we surveyed, nearly 60
20 percent have found the virus on their home computer at
21 least once in the past two years. Nearly 20 percent
22 have had that experience four or more times.

23 Ten percent of the respondents had experienced
24 computer damage from a virus or other type of malware,

1 and other questions showed that in a significant number
2 of cases, the damage could not be completely reversed. It
3 was either partially -- they couldn't fully repair it.
4 In some cases they couldn't repair it at all.

5 If you do try to project this to the hundred
6 plus million U.S. online homes, you can certainly say
7 nationally there are several million homes that have
8 experienced damage, I would estimate conservatively
9 hundreds of millions of dollars, if not billions of
10 dollars in repair costs over the last couple of years,
11 based on the cost estimates that people gave us. Also I
12 would say that millions of homes have lost data
13 permanently based on our survey.

14 As far as how these things get transmitted,
15 email, 62 percent of the people said they came by email,
16 but interestingly, almost 13 percent said it came from the
17 web or download from the web which is about one in
18 eight. That's kind of not as obvious a transmission.

19 User protection, 25 percent of the people had
20 not protected themselves against virus, either because
21 they didn't have anti-virus or they had manually updated
22 anti-virus, and they had not updated in the past month,
23 so that's a significant number of people that are not
24 following good practice.

1 I think just in sort of in summary here of what
2 the conclusions that I draw from some of this data is
3 that there's been significant economic and personal
4 damage already from viruses. Millions of consumers are
5 now sitting ducks for both hackers and viruses, and what
6 we see merely is that the federal and state governments,
7 which are supposed to protect consumers from what
8 essentially is crime, I don't think based on many
9 surveys I've done have taken the problem seriously
10 enough until this workshop.

11 For example, we had to do the survey because we
12 really couldn't find any kind of government data. Most
13 types of crimes now are tracked by the government, and I
14 think that's extremely important. In addition, as Dick
15 Clarke mentioned, ISPs being absent from the problem
16 solving, I think the government certainly has to get
17 involved at least to the extent of collecting data and
18 tracking the problem. We can't be substituting for the
19 government.

20 There's also -- despite that there are some
21 cyber crime laws, I found for the average consumer that
22 there's little meaningful law enforcement. If you're
23 hacked, even though there's a law against hacking, it
24 turns out if you're hacked in your home, if that

1 incident is not part of an interstate commerce or a
2 government or financial institution computer it's just
3 your home computer, basically the government does not
4 want to talk to you.

5 So, in summary, on behalf of the millions of
6 consumers, I think we can say that it's time for the
7 government to begin doing its job of monitoring these
8 crimes and protecting consumers.

9 MR. EICHORN: Thank you.

10 Larry Dietz, Larry is director of market
11 intelligence for Symantec, an information security
12 software and services provider. He's responsible for
13 market analysis, competitive assessments and strategic
14 directions and assists with business development.

15 Larry?

16 MR. DIETZ: It's always good to be like the
17 seventh speaker because you need to have a lot of
18 original material, and I'm mostly indebted to the FTC
19 for insisting that none of us use PowerPoint.

20 The first remark I would like to make is that we
21 need -- we must be very careful not to underestimate the
22 magnitude of trying to train, educate and inform the
23 average consumer of the problem.

24 I can recall several years ago when I was but a

1 young captain on assignment to teach communications
2 security to a National Guard unit. Sergeants came back
3 and said, Captain, we couldn't do our job. Why not,
4 guys? Well, sir, if we teach them how to be
5 communication secure, first we have to teach them how to
6 turn on the radio. And so the implication is most
7 consumers are not turning on the radio.

8 I'm also reminded, I worked for a company, we sold
9 computers to car dealers, and I did have to explain to
10 one of my customers that if you don't put chicken bones
11 in the printer, it will work better, so don't
12 underestimate the challenge.

13 First thing I point out is that the home is an
14 extension of the enterprise and that every employee is
15 also a consumer. As many of us work more than 40 hours
16 a week, we end up doing work at home. Home computers
17 get to be a target because they are an easier target,
18 and of course we've learned so far today that anti-virus
19 is not enough. I'm not going to repeat that.

20 I will mention the issue at home of multiple
21 users on the same computer which has not been
22 mentioned. Dick Clarke talked about the under three
23 year old. It is I think pretty clear that most young
24 folks are very technically inclined. Some of us still

1 have the double zeroes blinking on our video recorders.

2 So you have a class of users at home that I
3 would refer to as authorized users, unauthorized users,
4 and so individuals have to be cautioned as to who they
5 allow to use their system and what protection they take.

6 Employers have a clear duty to protect all entry
7 points to the information technology infrastructure.
8 However, they're not necessarily sensitive to that, and
9 new entry points crop up all the time, but there needs
10 to be an awareness of the need to commute, to telework
11 particularly in areas where the commute is very
12 difficult.

13 I was at a Gardner conference last week in
14 Chicago, and the figure they cited was that an employee
15 who commutes an hour who's able to commute or to work at
16 home, of that two hours, employer will gain two-thirds
17 of that time in increased productivity, employee gets to
18 keep a third, but there is more pressure to do that.

19 Next point I would make is that we're seeing a
20 blended threat where there is a blurring of the
21 difference between a hacker, a worm/virus,
22 malicious code, and an exploitation of the
23 vulnerabilities of the products or the configurations.
24 It was already pointed out that a lot of opportunities

1 exist for hackers because products are not updated.

2 In terms of threat vectors, the hackers are
3 doing port scanning. Some of you may find that there is
4 a fair amount of technical mumbo jumbo in dealing with
5 the Internet. Portology is one of my favorites. If
6 you're ever at a cocktail party with a ponytail person
7 and a baseball cap, you can say, Well, what about the
8 Port 80 problem, don't you think that's really
9 significant, and then take a sip of your drink because
10 that will be a little while explaining that.

11 In terms of the home, Dick did elude to the
12 point that the home is a target because it has a static
13 IP address. I know all of you study IP addresses, but I
14 think it's easier to say that it's harder to hit a
15 moving target than a stationary target, and that because
16 the home computers now have increased in power, they
17 become a more viable target, and obviously those that
18 are connected to broadband are paying \$50 a month, which
19 makes them even more of a target, and so there's a
20 filtering out.

21 We've also seen complexity increases in viruses, new
22 metamorphic viruses that change their patterns to avoid detection, as
23 well as the number of viruses.

24 I would also suggest that some of the future

1 threat will be team attacks, groups of decentralized
2 people, let's just keep pick a name at random, Al
3 Qaeda, that have cells in different places, all charged
4 with different acts, seemingly independent, unrelated,
5 but all with a common purpose.

6 Lastly, we were asked to provide some data to
7 the FTC in terms of things we found in the marketplace
8 based on research we've done and surveys we've
9 purchased. I can -- I agree very much with Jeff's
10 numbers. We found, the most recent research we have, 70
11 percent of users have an anti-virus of one type or
12 another, and only about 15 percent have a firewall.

13 In terms of how often do they update? It looks
14 like about half of them update automatically. It's also
15 done automatically over the Internet, 30 percent weekly,
16 about 12 percent monthly, and then about 3 percent each
17 for every few months after the virus, that's my personal
18 favorite, and never.

19 So in sum, working with the consuming public,
20 the small office, home office is going to be a difficult
21 challenge, and we have a long road ahead.

22 Thank you.

23 MR. EICHORN: Thank you, panelists. I think
24 this is a good time for a break this morning. Can

1 someone tell me what time it is according to that
2 clock?

3 Why don't we get back together about five of,
4 and this same panel will reconvene. Thank you very
5 much.

6 (Break in the proceedings.)

7 MR. EICHORN: Let's get started again. I just
8 wanted to remind everyone, once again, that if you want
9 to pre order your lunch sandwich, there may still be
10 time. I get a 10 percent cut from the cafeteria.
11 actually I don't.

12 (Discussion off the record.)

13 MR. EICHORN: I want to take a step back at this
14 point. We have a wide variety of attendees I guess, and
15 I just want to jump back to some really basic questions
16 for a moment, and I guess my first one would be: What
17 are the threats to consumers? Anybody?

18 MR. DIETZ: Well, the threats, as I mentioned,
19 are kind of a combination of hacks, which is an
20 intentional hostile act by a third-party, viruses and
21 worms, where code is received on somebody's machine,
22 either actively on their own part or passively, and
23 third, a vulnerability in the configuration of the end
24 user's machine, either because the products they have

1 are defective or because they failed to configure them
2 properly. Those are kind of the major buckets.

3 MR. EICHORN: Larry, can I ask you to describe
4 -- we've heard the terms viruses and worms and Trojan
5 horses is another one, and I'm wondering if you could
6 sort of define out what the differences are between those --
7 or whether that distinction matters to consumers?

8 MR. DIETZ: Well, I think as a practical matter,
9 the distinction doesn't matter. I had another one of my
10 famous clients say to me, The reason I hired you is I
11 don't know the difference between a megabyte and a dog
12 bite, so I don't think many consumers and small
13 businesses owners really care about what the problem is,
14 but I will help you out there a little bit.

15 A virus is a piece of hostile code that will do
16 something bad but must be activated by an act, and
17 viruses are typically one machine at a time, so when we
18 had the I Love You virus, it was a letter attachment to
19 an email, and the user had to double click on it, so the
20 user had to do something.

21 A worm, by definition, is self-replicating.
22 That means kind of like the wire coat hangers in your
23 closet, it makes more of itself, and you don't have to
24 do anything else, and the worms are particularly

1 dangerous because they can replicate themselves several
2 ways such as already has been mentioned, a download from
3 a web site, email, file sharing, disk sharing. Those
4 are all different ways that worms can self-replicate.

5 As far as a Trojan horse goes, everyone kind of
6 remembers the story about the big toy horsey that came
7 inside the gates, while on the outside it looked like a
8 really good thing, although why you would want an 80
9 foot horse is kind of beyond me, but it was really
10 dangerous on the inside. The payload in that case was
11 soldiers from the enemy.

12 You heard Dick Clarke talk about Code Red this
13 morning a little bit, and the nature of the payload was
14 such to take over the victim machine, sometimes called a
15 zombie in the jargon of the trade, and then use that as
16 a jump off point to attack a target, so that's a Trojan
17 horse.

18 MR. EICHORN: Thanks. Getting into sort of the
19 meat here, how are these threats changing? All of you
20 sort of mentioned this in some ways in your
21 presentations, but what are the factors that are causing
22 the risks to change? Rich?

23 MR. PETHIA: Let me go off on just a slightly
24 different direction for a minute because sometimes I

1 think the technical terminology that we insist on inventing
2 in this industry confuses some basic issues.

3 We all know about things like peeping toms and
4 voyeurs and vandals and thieves and organized crime.
5 Those aren't mysteries to us. We've heard about them.
6 We've dealt with them for years.

7 What's happening to us in the Internet and the
8 IP world is all those things are coming to cyberspace,
9 just like they've been in the rest of our space for all
10 of our lives, and one of the differences is they can
11 come with less risk because in order for a thief to
12 steal the money out of my house, he has to be physically
13 present, but for a thief to steal account information
14 from my PC, he could be sitting in Singapore just as
15 well as he could be sitting in my living room.

16 So distance begins to disappear when we get to
17 cyberspace. Time begins to get compressed. It takes
18 virtually no more time to access my system from
19 Singapore than it does from the house down the street.

20 So now all of a sudden you have to think about
21 not so much what are the technical threats, but what is
22 it that I have in my machine that someone might profit
23 from and therefore want to steal, or what is it that my
24 machine can do that someone might take advantage of?

1 For instance, we have reports from people who
2 have become unwittingly -- unwitting distributors of
3 child pornography because the bad guys found a
4 server on the Internet that was unattended and decided
5 they wanted to use it to distribute illicit information
6 rather than their own machines.

7 And then at the same time you have to think
8 about for all the people I do transactions with over the
9 Internet, what information have I given to them that
10 they have to protect, and what might the bad guys do if
11 they get their hands on that information?

12 So, for example, the thief who wants to steal
13 credit card numbers and information in order to
14 illicitly use those credit cards or sell them on a black
15 market, and there is a big black market right now for
16 that kind of information, is more likely to go to some
17 Internet provider of goods and services who has a big
18 collection of credit cards than he is likely to come to
19 me where I might find one credit card on my machine.

20 So I think when we think about threats it's
21 important to understand the technical nuances of how
22 these things happen, but I think it's more important to
23 recognize that this is crime. These are bad people
24 doing bad things for profit, and if you can think about

1 it in that way, it might help take some of the mystique
2 out of this and let people know that unfortunately we've
3 got to deal with criminals now in cyberspace just like
4 we've had to deal with them in the rest of our lives.

5 MR. LEATHERN: I think I would add to that that
6 I think we see people, the bad guys are going to be
7 going where the money is, and increasingly people are
8 accessing and having financial information available to
9 them.

10 The convenience factor is great. I can access
11 and conduct online banking transactions from my desktop
12 at work, from home, from on the road as I am now.
13 That's all great. However, there's a couple dangers
14 that exist and we're seeing.

15 One, a lot of compromises are happening if a lot
16 of systems are being attacked, if people's financial
17 information is being stolen or accessed without their
18 knowledge. This creates costs, costs not only to the
19 consumers themselves who are affected, but also costs to
20 companies. They will have to spend a lot more money on
21 security, and so they may not end up implementing online
22 access to their accounts. Consumers I believe to access
23 these convenient features will go away.

24 The other thing is you're also going to see

1 services be available but just not responded to so, for
2 example, if my email in box is stuffed with 150 SPAM
3 messages and a message from Citibank that my account
4 statement is now available online, it's increasingly
5 likely that I'm going to miss and have to pay that \$29
6 late fee because I didn't know that my billing statement
7 was there, so we're going to see something like that.

8 We're also already seeing a lot of social
9 engineering going on where people that create a virus or a
10 SPAM mail are employing technology to try to make it
11 look more -- look emails look more legitimate. This
12 makes it even more likely that the legitimate emails are
13 going to be confused or not responded to.

14 I don't know if any of you have received any
15 credit card solicitations recently, anyone? But things
16 like something that looks like a Fed Ex package, clearly
17 I'm going to open that because it looks important. I've
18 seen ones recently where some more poor schmo at
19 whatever the credit card company is signing their name
20 to make it look legitimate.

21 Those are the types of things we're seeing
22 online, and because the cost of sending email for
23 example online are so low and because you can get 10
24 million email addresses for 59.95 online, these things

1 are going to become increasingly more prevalent.

2 Our numbers indicate the average user received
3 about 500 SPAM messages last year. That number is going
4 to more than triple in the next four to five years, and
5 I think even that I think is a conservative number.

6 MR. EICHORN: Jeff?

7 MR. FOX: In the area of hacking, I think a big
8 change is the deployment of high bandwidth connections
9 with large numbers of ordinary home users, and that has
10 now -- because I think that hackers are after the
11 bandwidth, and the servers and corporate networks that
12 were targets were -- at least they had an IT staff.

13 Home users now have similar kind of bandwidth.
14 They don't have anywhere near the sophistication that
15 corporate networks do, and there are millions of them.
16 So it's like a million targets with no expertise with a
17 similar bandwidth.

18 And in the area of I guess viruses and malware,
19 when I was a software developer before I came a
20 journalist there was a slogan or saying that all
21 software proceeds until it's 90 percent complete, and
22 then remains 90 percent complete forever.

23 That's an essential problem we're going to have
24 to deal with, even with a lot of the problems we're

1 seeing, the bugs, I'm trying to think of the word that's
2 used for the flaws in the software, but the system
3 software, the operating systems, the Internet and client
4 software, they're not going to disappear.

5 They can tighten it up to a certain extent, but
6 given the proliferation of Internet applications and the
7 richness of applications, operating systems, powerful
8 processors, you're always going to see large complex
9 pieces of software, and I don't think you're ever going
10 to see -- I've never seen bugs disappear in 30 years
11 of using computers.

12 MR. EICHORN: Mary?

13 MS. CULNAN: One other thing that was mentioned
14 earlier but it's worth repeating here is it's easier and
15 easier for people to launch sort of unsophisticated
16 attacks because of the scripts and tools, and so you
17 don't look at the threat as being a monolithic thing,
18 but there are different kind of bad actors out there.

19 And certainly it's easier to deter the people
20 that are just sort of looking for somebody to hit and
21 want to use a pre scripted program to do it. Someone
22 who is a determined terrorist that really wants to get
23 at something in particular, that's going to take a
24 different set of tools, so I think that's also important

1 in thinking about threats as sort of break them into
2 who's interested in getting to what.

3 MR. HEIMAN: I think it's important to follow up
4 this idea of creating analogies to sort of the physical
5 world. I mean, you wouldn't buy a car, you wouldn't buy
6 a new car and then park it somewhere on, with the keys
7 in it, running and walk away. You sort of just wouldn't
8 do it, but in essence that's what you're doing when you
9 have a high speed connection. You're just leaving it on
10 all the time.

11 You wouldn't even buy the new car, leave it
12 parked and open and walk away. I bet you if we take a
13 poll right here, how many people, when they park their
14 car, lock it? Let's have a show of hands. Right?
15 Everybody does it.

16 Now, how many people have some sort of car alarm
17 that gets turned on? See, a lot but fewer. How many
18 people use The Club? See, there it is, and the numbers
19 go down.

20 I think we need to create sort of the virtual
21 analogies to sort of the physical world to really
22 educate people and really get it through, and much as
23 you have to take your car in every 3,000 miles to get
24 new oil or it just isn't going to work right, you have

1 to periodically get those updates on your security
2 features as well.

3 COMMISSIONER SWINDLE: Can I pose a question,
4 Jeff and Mary could perhaps deal with it and, Jeff, you
5 talked about it. It's slightly apart from this, but
6 it's all a part of securities and vulnerabilities,
7 talking about the software systems that come out, and
8 there's one big company in our world that recently came
9 out with a new product that Mary has, and it was
10 criticized by many.

11 And I'm concerned about -- we all know there's
12 no perfection in this. It's always revolving, searching
13 out bugs, making it better, and yet we have another
14 element now since the privacy debate has gotten so big,
15 and certainly the security debate is going to be big, so
16 we have a litigious environment now. We're going to sue
17 people, the developers, for bringing this on without it
18 being perfect because it has vulnerability.

19 Where is that taking us in this effort to
20 improve security or privacy? Is it going to be an
21 impediment or is it going to be an inspiration?

22 MS. CULNAN: Good question. You've obviously
23 let both of us speechless about this.

24 MR. FOX: You mean the litigiousness?

1 COMMISSIONER SWINDLE: It seems to me that all
2 the best minds and from every parameter that we can
3 imagine, countervailing forces, the civil society, the
4 industry, the public and so forth, we need to work
5 together as opposed to trying to take advantage of
6 others' fallacies, and obviously I don't think anyone in
7 the industry is seriously trying to create something
8 that's bad.

9 MR. FOX: But software companies need an
10 incentive. Until now obviously that incentive has not
11 been there.

12 MR. DIETZ: Let me just -- I'm licensed to talk
13 out of both sides of my mouth by the great state of
14 California. The products liability issue is a big
15 issue, but the products liability issue is, A computer
16 and its piece of software, is it like a gun? Guns don't
17 kill people, people kill people? Is it if I put a seat
18 belt on the car and you don't use the seat belt, is that
19 my problem as the manufacturer?

20 Mary pointed out she bought XP. She didn't know
21 it came with a firewall like capability, and it was
22 switched in an off position. Now, should the vendor be
23 made to ship product with an on position? Don't know.

24 MS. CULNAN: I think part of this is whether

1 we're speaking to sort of our individual interest as
2 either consumers or companies or to our collective
3 interests as a society, which is what Dick Clarke talked
4 about and try to find some ground where if it's clearly
5 in the national interest for companies to develop
6 software and tools and provide those easily to people so
7 that there is some form of protection, I think that's a
8 good idea, especially at sort of a rudimentary level
9 where maybe there can be some balance between something
10 that runs well versus something that doesn't and is
11 going to create an interest in people to sue.

12 COMMISSIONER SWINDLE: You harken back just a
13 few years, and let's speak of Microsoft, all the
14 problems that Microsoft had, although it's bringing all
15 these wondrous things that we now know as the Internet
16 and so forth and marvelous computing, and let's give
17 credit to Apple first because they came up with the
18 various and sundry means today that Microsoft uses, but
19 we joked about it.

20 Today lawsuits are being filed about it. Are we
21 elevating that aspect of this information technology
22 world to the point where it's becoming a detriment?

23 MR. DIETZ: Well, I think the litigation with
24 Microsoft is mostly about their trade practices, not

1 about the defects of the product.

2 COMMISSIONER SWINDLE: I am not talking about
3 the thing over here at the Justice Department. I'm talking
4 about current things, that it has vulnerabilities.

5 MR. FOX: I just want to speak as a former
6 software developer who's developed code. I don't think
7 the issue is so much whether people turn on a feature or
8 use a software. There's a question of the quality of
9 the software creation itself. The product, is it a
10 defective product, is it a quality product.

11 And when I developed software in the 80s, the
12 idea of a buffer overflow, which is one of the major
13 flows that have shown up in Microsoft software, we
14 didn't do that then. I honestly think that software
15 quality control is not what it was back then.

16 I think in the race -- first of all, software
17 has gotten bigger and more complex obviously, but good
18 coding practice in which you check for things like that
19 really honestly should have been in the Microsoft
20 software development methodology all along, and I don't
21 know why it wasn't.

22 Apparently now it is, but it took these problems
23 to get them to do that, but there's a question of
24 whether they are following good software practices, and

1 I think if a customer has shown not to have followed
2 good software practices, they've created a defective
3 product, and maybe there is a ground for legal action
4 there.

5 MR. PETHIA: I think the pendulum needs to swing
6 for awhile. There is probably as much new software in
7 my new truck as there is in my laptop, and yet I don't
8 have to stick my finger in that software every other day
9 to correct some flaw. Granted, it's not plugged into a
10 DSL connection, but there are literally millions of
11 lines of software and many products, and we know as an
12 industry how to produce those products with high
13 quality, high reliability, to ensure high availability
14 and good service.

15 So the question is: Do the quality features of
16 the product -- are they adequate for the marketplace
17 where the product's being sold? And I think today I
18 can't think of any vendor who could justifiably make a
19 statement that they don't understand the threat
20 environment of the Internet. People like SANS and CERT
21 and others have been publishing tons of data on what the
22 threats are, what the vulnerabilities are, what the
23 impacts of with all of these things are with respect to
24 secure, safe operation of computers so the vendors today

1 need to make a decision. Are they going to build
2 products that are fit for that marketplace or not?

3 I contend that a lot of products today aren't
4 released. They escape. They get out into the field
5 long before an adequate job is done of quality control
6 and testing and quality assurance, and that's something
7 I think we all need to make noise about, not necessarily
8 from a litigious standpoint, but we have to send a
9 signal to the vendors that says --

10 COMMISSIONER SWINDLE: That's my point.

11 MR. PETHIA: -- the quality of these products
12 today is just not acceptable given the threat
13 environment they're now expected to operate in.

14 MR. EICHORN: Can I jump in and just say we're
15 actually going to be discussing these issues a little
16 bit in a later panel that will actually be tomorrow so
17 we'll have more time to discuss this.

18 COMMISSIONER SWINDLE: Who says staff can't put
19 Commissioners in their place? Thank you for the
20 interruption.

21 MR. EICHORN: Could anyone on the panel comment
22 about other sort of issues out there like wireless and
23 file sharing? Larry mentioned a little bit, like Spyware
24 and Kazaa and all of these kind of things that are

1 out there and Instant Messaging as well, how are those
2 operating?

3 MR. DIETZ: There should be like a bell. If you
4 answer a lot of questions, we should get some money.

5 MR. LEATHERN: There is a lot of -- there are a
6 lot of applications out there. Some of them you refer
7 to Spyware. I think in most cases that refers to
8 something that's installed without your knowledge when
9 you're installing some other kind of application which
10 has legitimate purposes.

11 Also, I mean, there's a lot of -- there are many
12 applications out there that I say once they're on the
13 desktop, they may later be used for other purposes. It
14 also creates the ability to track what sites users are
15 visiting. For example, an example of this is Gator. I
16 don't know if many of you are familiar with Gator, but
17 it's actually really useful. It helps you remember
18 passwords at sites. All the information is stored on
19 your own computer.

20 However, obviously the way they make money is
21 they sell advertising so what they do is they'll pop up
22 windows every now and then that have an advertising
23 message, and if you're willing to put up with that and
24 occasionally click so that their advertisers stay happy,

1 you also get this application which lets you remember
2 different passwords at different sites.

3 The issue there is you have an application
4 that's on your system. It's sending information back to
5 the home base every now and then. Microsoft, when you
6 install XP, it's extremely hard not to sign up for a
7 Passport account if you don't have one, and they also
8 use it with the Windows Messenger product to keep
9 sending information back.

10 If you run Microsoft Word and it crashes, it
11 appears as though the problem is with your application,
12 click here to send a product, a message about the error
13 back to Microsoft, so there obviously is a lot more
14 information being traded by different applications.
15 It's not just your web browser that's accessing the
16 Internet. It's these other applications as well.

17 And once you, through your firewall, say, It's
18 okay for this application to access the Internet, it
19 then has kind of the ability to do so. Sometimes,
20 however, of course the good firewall products will tell
21 you if the program has changed since it last accessed
22 the Internet, so those are some of the things that can
23 help consumers here, but clearly the proliferation of
24 other products on the desktop clearly does make the

1 situation much more complicated.

2 MR. DIETZ: I have a couple of notes here.
3 First is wireless, anybody who uses wireless should have
4 no expectation of having security or privacy, period,
5 end of story, and particularly organizations with
6 sensitive data, and they don't have to be big ones,
7 let's take law firms. Law firms, we have a lot of egos
8 crammed in a small space, and they don't want to be
9 bothered. Wires are yucky things, how can you see my \$5
10 million desk, I want a wireless LAN.

11 So opposing counsel perhaps hires some nefarious
12 dirt bag or dirt bagette to sit outside in a truck and
13 just kind of listen to what's going on, so wireless, no
14 expectation of privacy.

15 Spyware, first question is who's the spy and
16 what for? The flip side of the workshop is privacy.
17 There is more than a little interest in the notion of
18 employers monitoring email. There's more than a little
19 interest of employers restricting what web sites, URLs,
20 universal record locators, employees can go to. Should
21 employers do that? Do employers have a duty to other
22 employees to monitor what their employees are doing? So
23 you have to look at who's the spier and what for.

24 The other thing is: Is it an advertiser that's

1 gratuitously sending up. Get a web cam. Is that a
2 problem, is that the spier, and was I one of these
3 brilliant individuals that gave my email address, my IP
4 address, my blood type, all for the chance at a \$25
5 raffle as we heard about earlier today. So who's the
6 supplier, what's the deal?

7 And last, but not least, Instant Messaging in my
8 view, and I would be interested in the view from CERT,
9 Instant Messaging is kind of like a VPN. It can be a
10 way that a secure facade such as an enterprise with its
11 firewall and so on, intrusion detection, is breached
12 because I'm Instant Messaging my sister on what we're
13 going to do for Aunt Ruthie's birthday, and that becomes
14 a way in for a potential attacker.

15 So all of these technologies have to be looked
16 at in context, and it's the duty of the business owner. It's the duty
17 of the parent to take the precautions to implement whatever policies
18 they want to set for their resources.

19 MR. EICHORN: Jeff?

20 MR. FOX: I would like -- with all the looking
21 at technology, I want to comment on again the importance
22 of looking at what some people are calling live ware
23 which are the human beings because you, the human being,
24 is the key. The user is the whole key here.

1 In one case talking about the file sharing and
2 Instant Messaging, I visited the Sub 7 site. That's a
3 site that actually distributes a Trojan called Sub 7, and
4 probably if you want to visit it should turn your firewall and AV up to
5 max I was warned, but there was explicit instruction there on what's
6 called social engineering, which was actually ploys and cons that you
7 could use when doing Instant Messaging with people,
8 chatting with people as to how to persuade them to
9 accept a Sub 7 Trojan that you would be giving them.

10 It was -- actually the person had written in
11 there kind of in their poorly written English, I found
12 lying works, and then gave actually arguments they could
13 tell people this was a video, this was a that. They
14 were actually coaching people on how to con people.

15 And the other aspect of live ware, about three
16 days ago, I received an email that I would call sort of
17 a human powered virus that would never be called by any
18 AV software or firewall. It was an email without an
19 attachment. I don't know if anybody else has received
20 it.

21 UNIDENTIFIED SPEAKER: Was it called deleting
22 and dealing and --

23 MR. FOX: It was very plausible. Consumer
24 explain what it was.

1 MR. FOX: The one I got had been forwarded by
2 about 50 different people, but the last person was
3 somebody I knew. Presumably they got it from someone
4 they knew so it was trusted and said that there was this
5 new virus floating around and gave instructions for
6 deleting this virus and that the virus software couldn't
7 catch it and that you were instructed to go actually
8 gave instructions, go to your start menu -- it actually go
9 into a certain place, delete the file, told you exactly
10 what the file name would look like.

11 I was sent this by a friend of mine who had
12 actually deleted this file blindly following -- you're
13 laughing, but you don't realize this is the level most
14 people are at, and I recognized it as a hoax
15 immediately, but this is more than a hoax for
16 these people who had actually followed this, besides
17 propagating it. They don't need to use the Outlook
18 address book.

19 They're getting the person to do the file
20 deletion, no need for a script kiddy anymore, and this
21 turned out to have been a minor Windows utility thing
22 that I don't think was important, but had that been a
23 company system file, you could have had essentially a
24 human powered virus that didn't require any scripts or

1 any kind of programming at all, and this is something --
2 cons have been with us since human beings began, and
3 this is not something that is a technological problem.

4 MR. EICHORN: When you look over the threats out
5 there and the trends, is there any trend out there
6 that's sort of in the right direction, that's making
7 security easier in any way?

8 MR. DIETZ: Well, I think when you buy a
9 computer, you get at least one AV program on there, and
10 you're free to choose either one or two or three or
11 however many. I think most new computers are shipped
12 with it. I think that's probably a good thing.

13 MS. CULNAN: As long as it's --

14 MR. DIETZ: It's different than the operating
15 system.

16 MS. CULNAN: I still want to argue that shipping
17 the software with the computer is a terrific idea, but
18 it's either got to be turned on or it has to be really
19 easy for people to it turn it on, and I'll give another
20 real world analogy. It's as if you bought a car, it came with seat
21 belts but the seat belts were hidden in a secret compartment in the
22 truck, and the only way you could find out how to get them out and hook
23 them up would be to read the entire user's manual.

24 It shouldn't be that hard. It should be easy,

1 and also people also need to know that they need to do
2 this, and that's even the harder task I think.

3 MR. HEIMAN: I'll say on the encryption front, a
4 lot of communications now are encrypted. When you're
5 shopping online, you look down and you'll see the little
6 lock, and SSL is being used. For folks using
7 Blackberries, the communications link is at least
8 encrypted using triple disk. There's lots of products
9 out there that can encrypt your stored data, but again
10 it's up to users to choose to employ those products.

11 MR. DIETZ: On one hand I think it's probably a
12 good thing that schools are starting to teach computer
13 skills as a part of growing up as early as the fourth
14 grade.

15 On the other hand, I can't be comfortable that
16 they're going to teach all the other things, adjust your
17 mirrors, fasten your seat belt, because most schools
18 tend to be pretty rushed, and I'm not convinced that
19 before all the little tykes go on the computers, they'll
20 hit their live update button or make sure that the
21 anti-virus is on, and I'm just a little concerned about
22 that personally.

23 MR. LEATHERN: I think a trend moving in the
24 right direction is I think recently we see a lot of

1 companies who when consumers are doing online
2 transactions, they're asking for additional information,
3 for example, asking for the card on the verification
4 field. It's that extra number on your credit card.
5 Recently I went to the gas station and I used my credit
6 card at the gas station. They asked me for my Zip
7 Code. That was something new that I had never seen
8 before.

9 So as you can -- as the technology improves, and
10 these databases are more available, they have access to
11 them in real time, they can do the -- they can match
12 your address to your credit card number. They can check
13 against a database that can detect if you're shipping
14 something to a known fraudulent or suspicious address.
15 If you try to make 15 different transactions in the last
16 30 minutes, they can look at your IP address and see if
17 your ordering something to be shipped to Florida when
18 you're actually accessing from Slovenia.

19 So technology is improving, helping on some of
20 these issues that I think especially in the
21 transactional area where money is definitely at stake,
22 there's a lot more investment going into that.

23 I think one of the areas where there's not as
24 much is just every day password practices and so on. I

1 think there's still a need for consumers to become the
2 bread and butter of how they think about interacting
3 with customers -- with companies, and I think the
4 psychology there is still -- it's still very different.

5 People see the Internet still as different, not
6 just another extension of the company they're doing
7 business with, and I think there needs to be an
8 evolution there as well.

9 MS. CULNAN: I think one thing where education
10 is also needed is that people just as they don't realize
11 that their broadband connected computer can easily be
12 scanned by someone looking for a place to attack, is
13 that there are password cracking programs that also run,
14 and if you have a password that's in the dictionary or
15 is too simple, basically you're putting yourself at
16 risk, and people don't know that so that's something
17 else along with adjusting the mirrors that needs to be
18 taught.

19 That's another thing when I poll my students periodically, and
20 too many people raise their hands and say, yes, their password is just
21 letters or it's a word that somebody could easily find instead of
22 having numbers and upper case and lower case and some
23 scrambled characters.

24 MR. FOX: I think that broadband enabled

1 computers, when they're sold, there either should be an
2 option to get a firewall or an option to turn the firewall
3 on. I don't know if computer manufacturers are
4 permitted by the antitrust settlement to reconfigure
5 Windows in that way, Windows XP. If they are and
6 they're selling the computer broadband enabled, then
7 they probably should turn it on by default, maybe not
8 for dial up users but certainly for people that have a
9 broadband computer.

10 Otherwise at least offer people the option of
11 getting a firewall with the computer.

12 MR. EICHORN: Mary just mentioned passwords.
13 Can you all opine on consumers' use of passwords and how
14 they do it?

15 MR. LEATHERN: I'll jump in because we did the
16 recent survey I mentioned earlier. Our survey done in
17 April found that 53 percent of users use the same user
18 name and password at substantially all or most of the
19 sites they visit. 25 percent of users write down their
20 password on this piece of paper that they keep right
21 next to the computer.

22 If you think about it, it isn't necessarily that
23 bad. If it's in your home, then it becomes pretty much
24 as secure as your home does, so depending on that. We

1 found about 7 or 8 percent of people use password helper
2 applications, either something like Gator, which is you
3 dial into your machine, all the information is stored
4 locally, or Passport -- Microsoft.NET Passport -- that with
5 participating partners all the information is stored on
6 servers ostensibly in Redmond, Washington, where you can
7 log -- you could for example log on to eBay using a
8 Passport account.

9 You wouldn't have to set up a separate eBay or
10 you would have to set up an eBay account but you can
11 then log on to it with Passport information.

12 So clearly there are people using the same user
13 names and passwords everywhere. Some sites have moved
14 away from letting you choose a user name so M. Smith,
15 obviously M. Smith will probably be taken so you're
16 going to have to go through a couple iterations until
17 you get to M. Smith 961 that works.

18 But then since I mentioned before many sites,
19 many consumers will willingly give out a user name and
20 password, register to receive access to a site so they
21 can get a \$100 sweepstakes, that's a problem because if
22 I'm using the same user name and password at the
23 Citibank site, I could set up a site to gather this
24 information and try to use it elsewhere on the web.

1 It's like having a door that everyone can stand
2 outside of for as long as they want and keep trying
3 different -- the 10,000 different combinations of the
4 typical house door key until they find one that works.

5 MR. DIETZ: I guess, once again both sides of my
6 mouth here. I think the notion of passwords is surely
7 important. Whether the user who uses the same one is
8 always at risk, I'm not willing to say. Password
9 synchronization can be a way for a user to use the same
10 password, presumably a difficult one.

11 I took an anti hacker class, perhaps the oldest
12 living graduate of said class, and we were told a really
13 good example is 100 percent milk. 100 percent sign M I
14 L K because it had numbers and it had one of the
15 characters and so and so forth, so users have to make
16 the decision on passwords that they can remember easily
17 and they have also have to manage them.

18 I've given up counting how many accounts and
19 things that I can't remember them, if someone is trying
20 to attack me, God bless them, if they gave me the list,
21 I would probably be happy about that.

22 I think you have to put things into perspective
23 and recognize the order of magnitude of the threat and
24 what's a common sense practice to defeat the threat.

1 MR. EICHORN: To what extent -- let's assume
2 that consumers are less sophisticated than businesses
3 are. To what extent does that affect how well they can
4 secure their own systems?

5 MR. PETHIA: This is a pet peeve of mine so let
6 me start with this one. We talked about quality issues,
7 and I think in addition to quality issues we need to
8 look at fitness for use from the perspective of matching
9 the product to the characteristics of the person who is
10 going to use it.

11 Today's laptop, desktops, the things we have in
12 our homes are very sophisticated electronic software
13 devices. Unfortunately, however, they're instructed in
14 such a way that the user has to have a lot of technical
15 sophistication to get both the power, but also the
16 security that's inherent in the products.

17 For years now we've talked about things -- we've
18 talked about, we haven't produced, we talked about
19 things called Internet appliances, things that are built
20 for the skill set of the people who are going to use
21 them. I think that's one of the big problems the
22 industry has to face over the next ten years.

23 If we ever want this big expansion and more
24 electronic commerce, if we ever want the trust of the

1 broad consumer base, the industry is going to have to
2 step up and build products whose characteristics are
3 matched to the characteristics of the people using them.

4 It starts very simple, from simple, easy to put
5 together, take out of the box, default configurations
6 and moves all the way up through things like
7 configuration management and worrying about whether or
8 not you have patches installed and getting virus
9 updates, all of that has to become two orders of
10 magnitude more automatic than it is today.

11 MR. FOX: I would like to mention a few things.
12 I interviewed a number of consumers in doing the
13 article. Not all of them made it into the article.
14 Once person I spoke to who had experienced some damage on
15 his computer from a virus and then had updated to the
16 new version of the anti-virus that he was using, this is
17 a question of lack of sophistication, is that at that
18 point he was bragging to me it was like perfectly safe
19 now to click on attachments and everything.

20 This is a guy who actually had experienced a
21 virus loss and even after having that happen, because of
22 his sort of total faith in the promotion of the product,
23 which told him how great it was, he now believed the new
24 version of course was perfect, and he didn't have to

1 worry about good practices anymore.

2 And although as a journalist, I'm just supposed
3 to ask questions, I couldn't help but give the guy a
4 little advice and say, Please, don't drop your guard
5 just because you have the new version, don't take it so
6 literally, but people trust this information, and they
7 have no way of knowing things like that.

8 MR. LEATHERN: I think one point I just wanted
9 to mention is it's hard to figure out whose
10 responsibility it is to educate the consumer in the case
11 of, when you're accessing your Citibank account on line,
12 knows the person who makes the browser, well it's
13 probably the same person who makes the operating system,
14 right, so is it Microsoft's job? Is it Hewlett-Packard
15 who made -- perhaps they made the PC. Is it the
16 software manufacturer that could have made the
17 anti-virus software. Is it Citibank itself?

18 A lot of things need to come together for this
19 to change, and the clients and the companies that I talk
20 to, it seems like everyone is waiting for someone else
21 to pick up the ball and run with it, and that's just the
22 thing that I see every day when I talk to companies
23 about these issues. It's great if VISA is spending
24 money or someone else is spending. I don't want to

1 necessarily be spending my own money in this environment
2 to educate the consumer.

3 MR. HEIMAN: It's everybody's responsibility. I
4 mean, I think it starts with parents and at the home.
5 You teach your kids to lock up when they leave the
6 house, and you teach your kids not to talk to strangers
7 on the street. You just have to incorporate that. The
8 school point was interesting, and I hadn't really
9 thought about that, but it's true.

10 Kids clearly are getting educated about computer
11 use at school, and I doubt they're incorporating any
12 security education as part of that, and that needs to
13 change.

14 Businesses are, need to, are doing more in terms
15 of educating consumers about the security features that
16 they are building into the products. So I think it's
17 really -- the short answer is everybody has to do more.

18 MS. CULNAN: I would agree with that, and you
19 need to educate the teachers that they need to educate
20 the students. It's fine to say, We need to teach the
21 students but if the teachers don't understand, and so I
22 think there's some real good opportunities to develop
23 some packages or summer institutes or other kinds of
24 things to get the word out there, and again if you start

1 young, then you don't have to worry about it so much as
2 people get older.

3 MR. EICHORN: From a practical side, this might
4 be best addressed to Jeff or Mary, but what happens to
5 consumers when you find a virus on your system? Where
6 do they go? What's involved in cleaning up?

7 MR. FOX: The first advice we give to people
8 is to disconnect from the net, and also don't do
9 anything immediately, I mean, because if you start to do
10 things or you try to delete it yourself or repair it
11 yourself, you're just going to get in more trouble.

12 These things are complex pieces of software and
13 many people naively assume if they just delete a file,
14 they've cleaned it or they may not even know if it's
15 actually a virus, but you want to run an AV scan as
16 quickly as possible, even if you have to go out and buy
17 it.

18 MR. EICHORN: We heard from Dick Clarke about
19 several interests of consumers. One is the role that
20 consumers play in denial of service attacks, and I guess
21 there are arguments that consumers have an interest in
22 protecting the network partly based on patriotism and
23 altruism and things like that.

24 But how do you think that consumers can be sort

1 of educated about the importance of security. Is
2 that -- so that there's a market for security?

3 MS. CULNAN: One way is it's in their own self
4 interest so they don't have to clean up after a virus or
5 some kind of a problem or worry about their identity
6 being hi-jacked, but the other issue I think is people
7 need to be made to feel, and maybe I'm being made to be
8 naive that this is going to be easy, but basically you
9 don't want to be the one that helped launch a terrorist
10 attack or created higher prices for everybody because
11 there were so many denial of service attacks that in
12 fact the costs do get passed on.

13 I don't know if there's some way to trace this
14 back to individuals. A few stories in the media perhaps
15 might get people's attention that ultimately you are
16 responsible, even if you don't get hauled into court or
17 go to jail, but basically it was your fault, but I don't
18 know. I think that's a hard issue, and we have to sell
19 that or it's not going to work.

20 MR. DIETZ: I think it's a difficult issue
21 because who is the consumer? Is it the person -- I
22 sound like the little red hen. Is it the person that
23 bought the computer? Is it the person that uses the
24 computer the most? Is it the person that's the default

1 computer support person, the person that's turned to in
2 the household when the computer goes cafluey? Just who
3 is the consumer?

4 MR. FOX: I would say anybody that uses email or
5 got on the net. I spoke to a woman who had a home
6 network and her son's computer which was on the home
7 network had been hacked by what she called hacker
8 vigilantes. These were people who actually found him
9 cheating on an online game, and they hacked in, deleted
10 this game which he had paid for, and so clearly
11 everybody in the household -- your kid is using sharing
12 files, downloading music and stuff like that.

13 If you think you're the user because you open an
14 Internet account, anyone using the Internet is a
15 consumer.

16 MS. CULNAN: It's sort of the same thing as
17 everybody who leaves the house should lock the door, so
18 I would agree it's everybody's responsibility.

19 MR. EICHORN: Several of you mentioned data on
20 how often consumers actually use like anti-virus, for
21 example. Does anybody have data on patching, how often
22 people patch?

23 MR. PETHIA: We probably have a lot of data on
24 how people don't patch, and we know that 80 to 90

1 percent of the security break-ins that we see could have
2 been prevented if people had upgraded their software to
3 include patches, and we also know most of those patches
4 are not for serious design flaws. They're for silly
5 implementation errors like buffer overflows.

6 So we've got lots of data that says the great
7 majority of incidents come from software that's not up
8 to date. The flip side of that though is it's really
9 hard when you have 5,000 new vulnerabilities being
10 discovered every year to make sure that your software is
11 up to date with the most recent hackers that were
12 probably produced three minutes ago.

13 MR. EICHORN: This might be a good time to turn
14 to questions from the audience. Just go ahead and
15 move up to the mike.

16 MR. LEATHERN: I just wanted to mention that
17 anyone that is interested in any of the data during any
18 of the comments I mentioned, just leave your business
19 card with me, and I'll email you a presentation that has
20 all of those numbers in there because I know a lot of
21 numbers are flowing around.

22 MR. EICHORN: If you do ask questions for the
23 mike, the court reporter has asked that you provide your
24 name. I'm going to leave that up to you.

1 MR. PALLER: Alan Paller from SANS. I was
2 taken with the discussion that Rich and Mary and Jeff
3 and Bruce had. Bruce's position seemed to be that users
4 should learn to do it themselves, but Rich said it's
5 like the seat belt's in a locked door, in the trunk, and
6 it can't be found.

7 And then Mary said it's outrageous that the
8 vendors would make it that hard, and, Jeff, you were
9 talking about incentives. What's the right incentive?
10 It's clearly not litigation. It might be litigation,
11 but it sounds awful to do it with litigation.

12 If it's not litigation, what will cause the
13 vendors to get it out of the trunk and make it
14 absolutely simple for Grandma to have a system that
15 isn't automatically attacked?

16 MR. FOX: Well, I think if things get so bad
17 that there's a ground swell of outrage and demand by
18 consumers, but I think we're still pretty far from that
19 I think, the market will always do it.

20 MS. CULNAN: Public humiliation I think.

21 MR. LEATHERN: I think it's ironic talking about
22 litigation. It seems people often get rewarded for
23 stupidity, spilling coffee on you or whatever. I don't
24 want to get into that whole issue, but to be perfectly

1 frank, people are -- you don't need to be -- you get
2 rewarded for that, and I think we're talking here about
3 people having -- being highlighted for doing silly
4 things when there's really -- there's an externality to
5 your actions.

6 You're not just allowing your own financial
7 information to be compromised or denial of service
8 attacks can influence everyone. I think it's a very
9 hard thing to do. I don't see an easy answer.

10 I think education and starting at an early age
11 are a good first step toward that, but the real answer,
12 should it be something like seat belts where everyone is
13 required to have certain software on their computers or
14 things configured in a certain way. I don't think
15 that's necessarily the answer. It's difficult to
16 answer that.

17 MR. HEIMAN: I think it's important to recognize
18 not only the severity of the problem but the complexity
19 of the problem too. I mean, what, at last count there's
20 some 50,000 viruses sort of on record now? You're
21 talking about 5,000 new vulnerabilities developed each
22 year to really acknowledge how complex these software
23 programs are.

24 So I don't think you can simply mandate certain

1 things. I think, in fact American industry is doing a
2 pretty good job of coming up with solutions and fixes
3 to things.

4 Now, I do think there is consumer responsibility
5 to use some of those tools, and if they use some of the
6 tools that are available today, then a lot of the
7 problem gets rectified.

8 MR. FOX: I want to say the biggest problem is
9 the lack of information about the number of, magnitude of
10 losses. When there used to be 50,000 people dying in
11 cars every year, that gave rise to Ralph Nader and the
12 consumer movement and movements to make improved car
13 safety.

14 And I think the reason that we don't see, as
15 Rich said before, yet a vigorous consumer advocacy here
16 is because we don't have the information. If people
17 knew hundreds of millions or billions of dollars per
18 year were being spent -- if people saw the numbers,
19 there would certainly be people then rising to the
20 occasion and then beginning to make the public case.

21 But in the complete absence of information about
22 what's happening, everyone knows what's happening on
23 their own little computer.

24 MR. HENNESSEY: Joe Hennessey with a

1 technology question. All of the threats that you
2 described, the viruses, the worms, et cetera, do they
3 all require the consumer, the end user to activate code
4 either by downloading it or double clicking it and
5 executing code?

6 MR. DIETZ: No. A number of the worms don't
7 require that at all. All the end user has to do is go
8 to a web site that has been compromised and poof, you're
9 hit.

10 MR. HENNESSEY: Are any of these worms
11 activated simply by opening an email?

12 MR. DIETZ: Viruses can be. Worms can be, yes.
13 Although I must say, any attorney who opens an "I love
14 you" message probably knew that was a mistake.

15 MR. KOENIG: This is Jim Koenig from ePrivacy
16 Group. As an attorney I have a question, but it's
17 actually for Rob and Jeff.

18 Rob and Jeff, in the data that you talked about
19 and discussed earlier, and I know there's a panel later
20 on about business models with respect to security, but I
21 want to ask a consumer perspective.

22 If in a general sense, whether it's confusion or
23 consumers don't know the difference or the market hasn't
24 pushed the companies to put it in the products yet, in

1 asking the question, who's interested in privacy, who
2 wants privacy, who wants security safeguards in place,
3 everyone will raise their hand.

4 If you ask the question, who wants the security
5 and is willing to pay an incremental amount more and
6 balance the two together, I think that's an operative
7 question, and that comes back to the market
8 determinations.

9 Companies see it's a differentiating factor.
10 It's a brand issue. If it doesn't tag them on their brand, it doesn't
11 affect the bottom line, then they're less interested.

12 So what type of data did you see there that
13 would help companies then be motivated to say, This is
14 an increasingly important financial issue for me that it
15 affects my bottom line, not just the interesting public
16 issue.

17 The second one is -- second question is on
18 consumer education, and so right now if consumers are
19 confused and don't know where to go and what to do, I
20 think we all have raised our hands and said that
21 consumer education sounds good. Who puts it together,
22 who finances it, who distributes it?

23 MR. LEATHERN: Your first question, I recently
24 completed a report about online privacy, and one of the

1 things I think always is a challenge to do is get away
2 from the abstract. For example, if you ask consumers
3 what's going to make them buy more stuff online, one of
4 the responses is better prices. Big surprise, 75
5 percent of people want better prices.

6 When you ask similarly about privacy and
7 security, I think you're always going to get a high
8 response rate if you say, I'm worried about my privacy.
9 I mean, in fact 70 percent of the people we surveyed are
10 concerned and they worry that their privacy is at risk
11 on the Internet.

12 However, the flip side of that is only 30 percent
13 of people actually ever read privacy statements online,
14 so what I think the challenge is is to quantify the
15 trade-offs that are made.

16 Are you willing to undergo something a little
17 more inconvenient, maybe spend another 30 seconds
18 signing up for a web site or providing a card number or
19 something like that to get the product or service that
20 you're looking for online?

21 I think businesses need to spend more time doing
22 that. We've been in a stage where in the last three or
23 four years we've seen companies throw traditional
24 business models out the window in order to try to get

1 consumers to buy things online or sign up for some
2 online account.

3 A lot of sanity has returned to the marketplace,
4 thankfully, so I think we see companies who have been
5 around the block and have been in business for 50 years
6 starting to try to get consumers to sign up for online
7 services, and that needs to be there.

8 Brand needs to be there. Trusted company --
9 companies with trusted brands are going to be able to
10 get consumers to sign up for their services. They're
11 going to be in a position to provide these services, but
12 they also need to ensure that through their privacy and
13 security policies they are retaining that trusted
14 position.

15 One thing I think is interesting that came out
16 of the report I just wrote is that I think companies are
17 doing a good job, need to take more credit for what
18 they're doing as well. They need to really -- I think
19 to call it marketing of their privacy policies, it seems
20 like kind of like an oxymoron, right, but they need to
21 take credit for things that they're doing well.

22 And I think by doing so, by going above and
23 beyond it, being within the spirit of laws and practices
24 and adopting best practices, that's the way we'll move

1 forward in this area.

2 MR. FOX: I want to say something about consumer
3 education. I was going to save this for tomorrow's
4 panel VII, but I don't know how many of you are staying
5 in hotels here. I found this in my hotel room, brought
6 it with me.

7 This is the campaign with that little dog on it
8 that you probably have seen in hotel rooms, the traveler
9 safety tips. I've seen this wherever I've traveled in
10 the country. This is a campaign, a crime prevention
11 campaign for travelers, people staying in hotels. I don't
12 know if it's a government/industry effort, but clearly
13 this is reaching people where it matters.

14 I just wanted to comment on the campaign that
15 was launched, the government/ industry campaign that was
16 launched during the winter which I thought was a great
17 idea, was launched with a lot of fanfare in February.
18 One of their things that they said they were going to do
19 was having twice a year when people turn their clocks
20 ahead and back, this was going to be like a check your
21 computer security thing.

22 The weekend of April 7 there was nothing. Just
23 to make sure I didn't miss anything I did a Nexis
24 search, and I found virtually no coverage since that

1 great launch in February, and so it looks to me at this
2 point that this campaign has not yet followed through on
3 its promise.

4 And it's not even a question of putting a site
5 up there and saying, We've got the site there, people
6 will go there. Ordinary people, people I know are not
7 hunting down sites like that.

8 You need something like this. You need
9 something where people are when they sign up for an
10 account or when they are getting their bills or
11 whatever. You need a place prominently all the time to
12 get in front of people's faces. That's the kind of
13 campaign you need.

14 MS. CULNAN: Also there's no such thing as a
15 giant consumer education program. This has to got to be
16 in chunks. I'm a big believer in small wins. I think
17 we can look at some other areas where there have been
18 some good efforts to educate consumers about problems.

19 Identity theft is one where the FTC and others
20 have done a terrific job being some place and pulling
21 out some of those postcards that you see when you go to
22 bars and restaurants and whatever. Then there was the
23 "don't let someone steal your good name" postcard from the
24 FTC, and I'm thinking this is really great.

1 So I think everybody needs to do their part, but
2 I think clearly one need is again to develop some
3 programs that get rolled out into the classrooms at all
4 levels K to 12. College, there needs to be curricula
5 developed that people can choose to use if they like it
6 or they can modify it.

7 And then everybody that's interested and
8 companies who have a little money and marketing insights
9 can step up to the plate and do their part.

10 MR. KOENIG: Just before I go, Rob and Jeff, was
11 there any specific data on consumer specific willingness to pay more?
12 I know Commissioner Swindle had the incentive of litigation or possibly
13 moving something, but was there anything specific about something

14 MR. PETHIA: Although I have to jump on that one
15 too. We don't expect to pay more for tires where the
16 tread doesn't separate from the tire body. We shouldn't
17 expect to pay more for software products where teenagers
18 or children can break in to them versus those being
19 very secure.

20 I think this is a basic question of, Are these
21 products fit for use in the marketplace in which they're
22 in, and I think today the answer in many cases is no,
23 and consumers shouldn't be expected to pay more for
24 products that are clearly advertised to work in that

1 domain.

2 MR. EICHORN: Last question.

3 MR. RONKEY: Bob Ronkey from Privacy Council, and
4 I'll tell you right up front that this question is going
5 to sound like I'm a heretic, but there's been a lot of
6 talk here that there's a huge problem and that there are
7 multiple components to that problem, whoever developed
8 the machine, whoever developed the software, who sold it,
9 who services it, and then us as users of it.

10 What I'm wondering about is, I've heard an awful
11 lot of talk how solutions exist, we just don't use them
12 so there's a motivation issue under that, that it sounds
13 like there's a lot of activity to try to motivate
14 builders of the software to make it better or the
15 sellers of the computer to make it easier.

16 So what the heretical question I'll ask is:
17 What motivates me as a consumer to take part in any of
18 your educational programs? I get an awful lot of
19 documentation with my software, but I go to the quick
20 start little sheet because I want to get going with it
21 right now, and I want to partake in the good stuff that
22 comes with getting online, but it will never raise to a
23 priority for me to truly understand some of the security
24 issues that are available to me.

1 So you've used car analogies a lot. If I go out
2 on the road and drive too fast, I get fined. If I don't
3 wear my seat belts in Illinois where I live, I get
4 fined. In the little town where I live 38 miles west of
5 Chicago, everybody locks their doors in my community,
6 but if I go another 38 miles west, there's a little town
7 where they don't because nobody goes there and they feel
8 secure so what's the motivation?

9 Should the solution -- Bruce said government
10 doesn't need to pass more laws, they exist. He said we
11 shouldn't mandate a specific solution because there are
12 multiple solutions, one of which might be better than
13 the other, but how do we activate the consumer? Should
14 there be the speeding fine or "you didn't use your
15 security" fine? I would be interested in what your
16 impressions are on that.

17 MS. CULNAN: Well, for one thing if we focus on
18 people who are younger than those of us in the room, you
19 basically have a captive audience, so they may choose
20 not to do it, but at least they're going to hear the
21 message because it's part of the curriculum and they're
22 required to listen. The older consumers, it's a harder
23 sell I think.

24 MR. FOX: I do object to putting the onus on

1 the consumer, even though the consumer has
2 responsibility. I think that just simply saying it's up
3 to consumers to protect themselves, it's dealing with
4 street crimes by saying, Okay, everyone is going to wear
5 Kevlar vests.

6 You have to deal with the roots of the crime.
7 You have to deal with -- the essential problem is the
8 Internet's infrastructure was not built for the kind of
9 activity that's going on now, and ultimately it's the
10 Internet's own mechanism, they're going to have to
11 create traceability, accountability and better security,
12 control the Internet itself because that's why you can't
13 track down the people that hack into your computer.

14 That's a long-term problem. We're dealing even
15 with AVs and firewalls with really short term issues of
16 to wear the Kevlar vest while the bullets are still
17 flying, but long-term we have to find some way to stop
18 those bullets from flying.

19 MR. HEIMAN: Well, I wear seat belts because
20 when I took driver's ed way back when, they showed you
21 gruesome photos of people who didn't. My kids wear seat
22 belts because if they don't click up, we don't leave the
23 driveway. I think that sort of the captive audience
24 point is the right one.

1 I think you sort of answered the question. In
2 your town everyone locks their door because they
3 perceive a threat, and 38 miles away people don't
4 because they don't, and I think what we need to -- so it
5 comes back down to the education point which is those
6 people in that other town where they don't lock their
7 front doors, if they get online, they have to feel
8 threatened.

9 They have to know that there's a risk out there,
10 and so I really do think it begins with sort of basic
11 education and it begins with the family and parents.

12 MS. CULNAN: Jeff's point about if there were
13 more data available about what can actually happen to
14 you in a tangible way if you don't implement, sort of the
15 gory picture kind of thing, that might help too. I
16 think people don't perceive there's a problem, a lot of
17 people don't.

18 MR. LEATHERN: I think another captive audience
19 that you can have is companies, if a company -- we've
20 talked a little bit about how it is good practice for a
21 company to tell its employees about these things, and
22 you can start there again. I mean, I spoke with
23 Hewlett-Packard, and they have a web based training
24 system that tells their employees how they should be

1 treating customer information, how they should be
2 respecting their customer's privacy.

3 That's a great place to start if you start with
4 big companies and give them encouragement, maybe money
5 or there's obviously a number of different ways it
6 could work. But it's a great place to start, and I
7 think we need to start there as well as start with the
8 younger consumers, the consumers who -- it was funny, about
9 a year ago we did a survey. We asked teens and their
10 parents who thought they knew more about the Internet,
11 and 97 percent of teens said they knew more about the
12 Internet than their parents did, so clearly that's a
13 great place to start.

14 MR. EICHORN: Well, can I -- oh, I was going to
15 cut it off. Rich, you want to make a quick point?

16 MR. PETHIA: One other quick one. I'm very
17 happy to see the June issue of Consumers Reports because
18 those of us in the security business have been talking
19 to each other for years, and we have to get this message
20 out to people in vehicles that they already relate to.

21 And the more we can do with Consumers Reports
22 and other kinds of consumer publications, events, to get
23 this message to an audience in a vehicle that they're
24 accustomed to dealing with, the sooner I think we build

1 that awareness that causes people to want to take some
2 action.

3 MR. EICHORN: We've been running about 15
4 minutes late all this morning, and I want to continue
5 running 15 minutes late so we don't cut into the lunch
6 break, so why don't we start after lunch at 1:15.

7 There's a list of restaurants that are nearby in
8 your packets, and I really want to thank the panelists
9 from coming from all over.

10 (Applause.)

11 (Whereupon, a lunch recess was taken at 12:00
12 noon.)

13

14

15

16

17

18

19

20

AFTERNOON SESSION

21

(Resumed at 1:15 p.m.)

22

PANEL II: What steps can consumers take now to secure
23 their information? What are businesses doing to
24 education consumers about these steps?

1 MODERATOR: LAURA BERGER, Attorney, FTC

2 PANELISTS:

3 TATIANA GAU, Vice President, Integrity
4 Assurance, America Online, Inc.

5 STEPHEN C. JORDAN, Vice President and Executive
6 Director, Center for Corporate Citizenship, U.S. Chamber
7 of Commerce

8 SHANNON KELLOGG, Vice President, Information
9 Security Program, Information Technology Association of
10 America

11 CHENGI JIMMY KUO, Network Associates, Inc.

12 BERNHARD MEISTER, Systems Architect, Security
13 Architecture, Development and Implementation, Verizon
14 Communications

15

16 MS. BERGER: Good afternoon. I would like to
17 ask everyone to please take your seats so we can begin
18 the first afternoon panel.

19 I'm Laura Berger. I'm an attorney at the
20 Federal Trade Commission, and this panel is about
21 consumer information security education and what steps
22 consumers can take now to secure their computers. We
23 heard some about that this morning. I think the
24 discussions naturally blend together that way.

1 This panel is only 45 minutes, and we're going
2 to allow ten minutes towards the end for questions.
3 And because of the brevity of the panel, I've asked each
4 of the panelists to just be prepared to do a dialogue
5 about this topic, so I'm going to quickly introduce the
6 panel, and then we'll start talking.

7 Immediately to my left is Tatiana Gau, senior
8 vice president for integrity assurance at AOL.

9 Continuing down the line we have Stephen Jordan,
10 vice president and executive director, The Center for
11 Corporate Citizenship at the U.S. Chamber of Commerce.

12 To his left we have Shannon Kellogg, vice
13 president, information security program, Information
14 Technology Association of America.

15 We have to his left Jimmy Kuo of Network
16 Associates, Incorporated.

17 And on the far left, my far left we have
18 Bernhard Meister, systems architect, security
19 architecture, at Verizon Communications.

20 So to start our discussion of what consumers can
21 do now to secure their own computers, let's talk for a
22 minute about the top ten tips. We heard a little bit
23 this morning about what are the top five things or some
24 of the important things people consumers can do to

1 secure their computers.

2 What are the most important, the top ten things
3 that consumers can do? This is on a volunteer basis.

4 MS. GAU: I'll jump in. I'm going to try to not
5 be redundant on some of the points that have already
6 been covered earlier today, and I'm going to go down to
7 the basic level of talking about the average consumer
8 out there and not the user who is already on broadband
9 and has a certain higher degree of sophistication I'll
10 call it.

11 We recently did an Internet study which actually
12 was part of the launching pad for the Stay Safe Online
13 campaign that was launched in February as was referenced
14 earlier today, and we interviewed Internet users at
15 large from the most novice level to a higher degree of
16 sophistication.

17 And we clearly found that people just are not
18 taking the proper precautions that they should be. 77
19 percent of users indicated that they did not update
20 their anti-virus software on any kind of regular basis.
21 They are not using strong passwords such as alpha
22 numeric combinations or passwords of a length of six or
23 more characters, so it really was kind of a level set
24 there that I wanted to establish with respect to the

1 type of consumer that I would like to talk about today.

2 In that context, the top five tips that I would
3 throw out is: Number 1, and this is something that we
4 reinforce through various means on the AOL service by
5 communicating with our members through messaging that we
6 provide online, alerts that we provide to our users when
7 they sign up, sign online for a session, specific areas
8 on the AOL service that we promote and push members
9 into, help areas and things of that sort.

10 The first number 1 tip that we push right now is
11 to have a strong password, right from the outset create
12 a password with a combination of alphanumeric and make
13 it at least six characters long or more preferably, but
14 those are the guidelines that we put out for passwords.

15 Second item, make sure you have anti-virus
16 software and keep it up to date, obviously emphasizing
17 the latter point as we've already seen and discussed
18 today.

19 The third tip that we always give to our users
20 is to notify AOL, and this really serves as a central
21 point for the flow of communication and understanding of
22 the issues that are impacting our users because by our
23 members notifying us of problems that they encounter
24 online, scams that they are seeing happen online,

1 viruses that they may have received, it allows us to
2 take steps on the back end from the technology
3 perspective as a business, where we protect our network
4 and protect our consumers before the problems even land
5 in their mailbox.

6 It also provides a way for consumers to reach
7 out and get help in certain situations, and we have
8 Notify AOL Buttons scattered all over the AOL service in
9 the mail read form, in the Instant Message form, on the
10 AOL web site areas, in the chat rooms, on the message
11 boards so that wherever something could possibly happen,
12 members have a quick and easy way to notify us about it.

13 Going on down the line, I would put using firewalls
14 to protect yourself if you're on a high speed
15 connection and also to make sure you download security
16 patches, of for a more slightly
17 sophisticated user unfortunately.

18 In the same survey that I referenced just a
19 moment ago, we found that less than 30 percent of the
20 respondents of this survey said that they downloaded
21 security patches on a regular basis, and remember, this
22 is obviously self attestations so the number is probably
23 actually lower than that.

24 But another question in the survey asked how

1 they learn of security issues, how did they learn of
2 patches being released or how did they learn of new
3 viruses or things of that sort, and overwhelmingly
4 people said that they got their information from
5 television, and most interestingly, of the respondents
6 that had seen some message relating to security, the
7 vast majority of them recalled a virus alert of some
8 kind, and that really was the message that they were
9 getting most often.

10 Finally, the tip that I would put out here is
11 the tip that we always give to consumers no matter what
12 age they are, whether they're adults or whether they're
13 children, don't give out information gratuitously.

14 For children, it's obviously important for
15 parents to teach their kids not to talk to strangers,
16 don't give out personal information, things of that
17 sort, but the same rule applies to adults, and we find
18 that a lot of consumers have a false sense of security
19 in some ways in their homes.

20 Their door is locked. They're comfortable.
21 They're in comfortable clothing. They're sitting at
22 their computer. And caution just doesn't seem to play
23 the same role that it would play in some other setting
24 than when they're at home, and with that I'll turn it

1 over to somebody else.

2 MR. KELLOGG: One thing that I would add there,
3 and those are all excellent steps to take as a consumer
4 and for small and medium sized businesses, remember I
5 think from the outset that we need to reiterate probably
6 what we said this morning, that this is a continuous
7 process.

8 So any of these actions that Tatiana is
9 recommending for consumers or small businesses has to be
10 done on a regular basis, or ultimately you're not going
11 to get the results that I think we're all looking for.

12 Another thing in, this area of broadband and
13 hopefully as we go forward with more broadband
14 deployment, remember to disconnect from the Internet
15 when it's not in use. That's also something important
16 to remember as far as specific actions.

17 And then kind of looking again sort of at a more
18 general level, we at ITAA work a lot with our larger
19 corporate members and also a lot of our security
20 vendors. We've got 140 companies that are involved in
21 our information security, many alone, and we do a lot in
22 trying to get the issue of information security up at
23 the board level and making sure that businesses look at
24 it as a business continuity issue, not a business

1 survivability issue.

2 It's the same message to small and medium sized
3 businesses and an important part of our audience for
4 today as well as the average consumer in that we want to
5 make sure that they look at this and understand
6 information security as a business continuity issue, if
7 not a business survivability issue.

8 And therefore there are a number of things which
9 Tatiana has already gone over that you can do that are
10 free, that don't cost a lot of money because we
11 understand whether you're a home user or if you're a
12 small or medium sized business, that you can't
13 necessarily invest a lot in this area, but there are
14 things that you can take, are steps that you can take
15 that are basic and are forward looking and can start at
16 the consumer with this.

17 MR. KUO: First of all, if you didn't pick up
18 this thing this morning, there's a whole stack of them
19 outside. This is my paper that was written for Stay
20 Safe Online campaign and as the anti-virus presentation
21 for that campaign.

22 But one more thing that businesses can do is
23 that when they have service online, they should find or
24 realize what those machines are there to do and limit

1 the machine down to only those services, so if you're
2 not supporting FTP, turn all those things off.

3 If you're not supporting Telco on that machine,
4 turn all those things off, and it's a matter of
5 education, but it's much safer to only allow those
6 things that that machine is going to do to only allow
7 those services.

8 MS. BERGER: I want to interject for one
9 second. You mentioned something that businesses could
10 do. Is that something you would advocate for consumers
11 as well just to set their computers for how they're
12 going to be used?

13 MR. KUO: For home users, generally they should
14 have a firewall, a personal firewall, and if they
15 don't turn off their machines and get off the Internet
16 when they're not using it, they should at least turn
17 that firewall to the high setting so that when they're
18 not using it, all the ports are closed.

19 MR. MEISTER: I would just like to amplify on
20 the comments made certainly so far in that what we're
21 seeing is the redeployment of computers in the household
22 more in the aspect of data centers. If everybody were
23 to regard their laptop, their home computer more in the
24 form of this is my family, this is -- within this

1 machine is my family's jewels, my bank account
2 information, my resume, my -- all these very sensitive
3 family documents, we have to start to separate.

4 That's one thing I would advocate people to do
5 would be to separate family data away from the devices
6 within the home that will be going on to the Internet on
7 a frequent basis. I know in my house, my son, he has
8 his desktop machine.

9 I make sure all our family's information is on
10 our secured server we have in our living room, it's a
11 mess in there, but this is the concept though. We have
12 to take it to the next level, be able to say, Okay, a
13 firewall is an essential. I would say firewalls
14 today, even if you are on a dial up connection, I'm
15 starting to see people talking about -- actually I've
16 seen personally scans coming through dial up
17 connections.

18 So the broadband issue will only exacerbate the
19 vulnerability to the home environment, but
20 unfortunately, we have a home environment where the
21 parents are very busy, very frustrated about all this
22 new technology. Their children are developing skills
23 which they don't understand, and it's a very tough call
24 for the parent, so my message really is to not only

1 focus on the PC and your home computing environment,
2 it's no longer just a PC.

3 You have PDAs, you have wireless, you have
4 infrared, all these elements can combine together, but I
5 would also emphasize that we have to do better as an
6 industry in demystifying how these things work.

7 I think too often we throw up our hands and say,
8 Oh, I don't know how this works so you don't do
9 anything. That's really running away from that issue.
10 And I would like to see demystification become part of
11 our dialogue between our consumers and those who provide
12 the technology.

13 MR. JORDAN: You know, when you originally asked
14 the question, it was about the top five security tips.

15 MS. BERGER: Actually it was the top ten, but
16 it's gotten narrowed down as we've again down the line.

17 MR. JORDAN: I think what we need to do is we
18 need to make a distinction between behaviors and tools,
19 and a lot of folks talk about tools, firewalls,
20 software, anti-virus packages, things like that.

21 And I think that one of the things that Shannon
22 was getting at is behaviors are just as important for
23 this, and one of the things about this too is the tools
24 and techniques are probably going to change and evolve

1 and are going to be very dynamic, and I think that sites
2 like Stay Safe Online and things -- and other web sites
3 and other tools that keep track of the tools are going
4 to be very dynamic on the tools part.

5 But I think that the basic behaviors need to be
6 filtered out as well, and then those need to be
7 disseminated, and that doesn't necessarily have to be
8 that evolutionary. I think that basically talking about
9 applying your elements that you apply for physical
10 safety to your cyber safety posture is something that
11 maybe we can educate a mass audience about and probably
12 they can make their connection very quickly too.

13 MS. BERGER: So we're starting to talk about
14 this in terms of getting consumers to understand the
15 process. I just want to follow up on something Bernhard
16 was telling, if other people want to comment on this,
17 about getting consumers to understand what of their data
18 is sensitive and to target that data and protect it.

19 I wondered if other of the panelists had
20 thoughts on that.

21 MR. KUO: Another comment about what small
22 businesses can do, one of the biggest problems on the
23 web is when you give the credit card to the company that
24 you're doing business with and you find out later that

1 it's been kept on an unsecured server and that whole
2 database was just compromised, and that's one of the
3 things a business can do is to take that credit card
4 database off of that web computer and put it on simply
5 another computer that's not on the Internet.

6 And that computer is the one that does all the
7 billing and is only dialing out to do the billing, but
8 if you looked at what are the crown jewels of the
9 business, and that set of credit card numbers is really
10 critical, just take that off and move it off to the side
11 or to a more secured server.

12 MS. GAU: I'll try to take a stab at your
13 question, Laura, in terms of what can consumers do with
14 respect to data that they have on their computer in
15 their home.

16 One of the tips that again is part of the
17 National Cyber Security Alliance's efforts is to make a
18 back up of your computer data, and there is certain
19 advice that's provided in terms of how often you do that
20 and how far away you should store that from the computer
21 so it's not right next to it.

22 But I think that that is something definitely
23 that consumers are not doing on a regular basis. It
24 doesn't protect the data obviously if the data gets

1 stolen, but it addresses a situation such as a virus
2 infection where important files get deleted.

3 To the issue of actual protections for people's
4 data on their computer, I'm going to actually echo my
5 colleague's comments with respect to behavior. I think
6 that there are tools out there that consumers could use
7 if they wanted to, to encrypt their data on their
8 computer or, for example, use firewalls and things of
9 that sort.

10 But ultimately it is about behaviors and making
11 sure that consumers understand the need to do this, and
12 interestingly enough, one of the approaches that we took
13 earlier this year with this alliance was to call upon --
14 we actually called it the Call to Action.

15 As a citizen of the United States it is your
16 duty to do your part in trying to protect the nation's
17 infrastructure. Yes, there's other elements that need
18 to play a role in protecting our nation's
19 infrastructure, but you as a consumer need to make sure
20 that you don't unwittingly become the mechanism through
21 which an organized group or a disorganized group could,
22 in fact, attack a government web site or some other
23 system in our country by having your computer become a
24 robot simply because you had a password that was too

1 easy to guess.

2 And we found that really using that kind of
3 approach as a call to action just as we need your help
4 to be on the outlook -- to be on the look out for things
5 happening in your neighborhood, and currently of course
6 with the latest terrorist threats that have come out, to
7 be vigilant for what is going on in your apartment
8 building, for example, are these people coming and
9 going, what is going on.

10 The same thing applies to the online world, and
11 it's a message that hasn't really come across that
12 strongly at this point, and it's one of the things that
13 I think may well be a driving force to getting more
14 people to pay attention.

15 MS. BERGER: Just -- go ahead.

16 MR. KELLOGG: I was going to say, that's what I
17 like about Stay Safe Online, if I may just be blunt, is
18 it boils things down so everyone can understand what
19 we're talking about, and it also pulls a lot of
20 different resources together.

21 Sometimes these can be very complicated issues
22 but some of the steps you can take are very simple.
23 Stay Safe Online does that. It packages things very
24 easily so you can understand it, and what it does and

1 what we're all talking about here is it sort of
2 addresses this issue of establishing a culture of
3 security which our friend Commissioner Swindle talks a
4 lot about, developing a culture of security.

5 Now, you want to do that in your home. You want
6 to do that in your small business. You want to do that
7 in your corporation. You want to do that in your
8 organization. You want to do that in government, and
9 it's key that we have this mentality.

10 This is our responsibility to do that, whether
11 we're at home or in small businesses or in corporations,
12 and again Stay Safe Online pulls that all together. I
13 think that's more important, and we should be supportive
14 in industry as well as in the public sector and of
15 consumers or from the consumer standpoint of initiatives
16 like this and get aware, understand what's out there
17 already, and so we're not reinventing the wheel, and
18 most importantly we're not making things more
19 complicated than they already are.

20 MR. JORDAN: I think there's a part of this that
21 we should also look at, which is while there are
22 fundamental base line behaviors that would apply to all
23 consumers, that not all consumers are monolithic, that
24 you don't have -- you might have some fundamental

1 things, and then each category of consumer is also going
2 to have specific needs that should be tailored to their
3 particular interest.

4 Under Stay Safe Online right now, what we're
5 seeing is that we're getting predominantly to new users
6 and to heads of households and to small business owners,
7 and --

8 MS. BERGER: Stephen, I'm going to pause you
9 right there, because before we get into -- this is a
10 very important discussion we're starting to have about
11 alerts for consumers and Stay Safe Online and how you can
12 tailor education efforts to the appropriate consumers,
13 but there are just a couple more areas of tips to
14 consumers that I want to hit first before we move on and
15 pick up with that discussion.

16 And one is an implication of something that
17 Tatiana has just raised, which is maybe getting
18 consumers to recognize when someone has or is attempting
19 to interfere with their systems. I would like to know
20 if the panelists think that that's also an area for
21 consumer education, getting consumers to recognize when
22 something has gone wrong with their system so that they
23 can repair it or intervene and fix it.

24 MR. MEISTER: Is this microphone working? This

1 morning it wasn't working quite that well. I just want
2 to take your point because it is important to see that
3 part of that process is to understand, and I'll give you
4 an example.

5 We have a home network. My son was chatting
6 online, and I personally find as a parent I don't like
7 him talking to strangers. Who was he talking to? Well,
8 I'm lucky I do have some knowledge of the security
9 realm, so I put on a packet sniffer, and I began
10 sniffing packets. Now, the illustration here is not
11 that I spy on my son. I trust him implicitly.

12 COMMISSIONER SWINDLE: Verify, right.

13 MR. MEISTER: But I wanted him to see
14 categorically how easy it is to sniff this information
15 and how non anonymous it truly is, so it's through these
16 small illustrations, these small lessons, if you like, I
17 also did the same technique with my own management. I
18 showed how VPNs worked by throwing something going
19 across in the clear, including budget information which
20 was of course fictitious, we have no budgets, money,
21 terrible.

22 But to see important information in the clear
23 being deciphered out of this wire to me is a very
24 important lesson in understanding, and this is why

1 perhaps I feel like a broken record here, but when we
2 talk about firewalls, my firewall goes off
3 continuously because I see people trying to do stuff.

4 Some of it is very innocent. Some of it maybe
5 isn't, but the next generation firewall hopefully will
6 be able to combine some of these aspects.

7 MS. BERGER: So you're suggesting one of the
8 ways that consumers can be alert as to something that
9 might be going wrong with their system is through firewalls
10 that give them notifications.

11 MR. MEISTER: Absolutely.

12 MS. BERGER: I just want to see, are there other
13 important ways that consumers can be educated about how
14 to recognize if something has gone wrong that they need
15 to remedy to people.

16 MR. KUO: Go ahead.

17 MS. GAU: Are you sure?

18 MR. KUO: Go ahead.

19 MS. GAU: One of the things we try to do at AOL
20 to help our consumers recognize problems, particularly
21 in the variety of malicious web sites or viruses, Trojan
22 horses and scams for that example is actually put up
23 examples of what these things look like online.

24 We have an area called the Neighborhood Watch

1 where we post alerts about the latest virus that is
2 going around and what the email looks like when you get
3 that virus. Normally when a virus first hits oftentimes
4 it's appearing as the same email. Of course that
5 doesn't last very long because then it starts mutating,
6 that is, the email that is carrying the virus has an
7 attached file, but also with web sites, fake store
8 fronts so to speak.

9 There's a big problem right now with bad guys
10 creating look alike web sites for top named companies on
11 the Internet, sending an email saying, You have won this
12 that or the other and you'll get 25 percent off your
13 shipping to come here, log in, boom they've got your
14 password. In some cases they get your credit card too.

15 So we will put up examples of those kinds of
16 sites online, and we give the step that always navigate
17 to a place where you're going to be giving personal
18 information by typing in the URL. Don't go to that web
19 site by clicking on a hyperlink in a piece of email that
20 you don't know where it came from and you don't know
21 whether or not that email is authentic. The safest way
22 to make sure you are at a legitimate web site and giving
23 out the right information is simply to manually have
24 typed in the URL.

1 MS. BERGER: Because this is a short panel to
2 begin with, I'll go ahead and let you all move into
3 giving the highlights of the important consumer
4 education efforts that are out there, and if you want to
5 address at the same time what you have found through
6 your experience the level of consumer awareness to be,
7 feel free to comment on that as well.

8 We've already talked a little about Stay Safe Online.
9 I don't know if people want to pick up with discussion
10 of that.

11 MR. JORDAN: I was just going to go through and
12 say that we are finding that there are very different
13 user sets on the Stay Safe Online set, and it basically
14 breaks down into about six categories. The first of
15 course are the new users who -- their kind of feedback
16 is, I believe somebody is trying to scam me, how do I
17 report them, I really appreciate your site, but I'm
18 having trouble getting out of it, can you send me email
19 with information about it, but you know early
20 adopters -- I mean, early to the process and are really
21 trying to figure out the stepping stones of how this
22 works.

23 The second group, the parental group, is very
24 traumatized by pornography and by viruses and by scams,

1 and they're really looking for information about access
2 issues.

3 The third group are the functional users, the
4 small business owners. The kind of questions that they
5 have for us are -- it's like a little bit of a higher
6 level of education, and they're really looking for
7 vendor education, for determining preferences. They
8 would like to know, for example, what firewall works
9 better than another or is there such a thing as a
10 spaminator or things like that. That was a cute quote.

11 But anyway, then another group are the truly
12 technological users, and what's interesting about their
13 behaviors is that they seem to divide into three
14 different subsets. One subset is rather complacent
15 actually, and they feel like they've got all of the tech
16 tools. They know what's going on. They don't think
17 that they're really vulnerable, and they don't see what
18 all the fuss is about.

19 The second subset that we're seeing are the true
20 believers, the folks that have one set of hardware or
21 software solutions that they think is better than
22 another, and they've got a set of preconceptions, and I
23 think, Jimmy, you can talk a little bit to the religious
24 force there a little bit later.

1 And then the third set are the activists.
2 They're the folks that know about the threats, know
3 about the vulnerabilities and want to see action done,
4 and they actually want more information about the
5 process behind security, so these are some of the things
6 that we're really seeing in terms of the customer
7 profiles or consumer profiles.

8 MS. BERGER: Given the segmentation that you're
9 describing, what are the ways, the best approaches to
10 educating consumers? They're using the Internet for
11 different things and they have different levels of
12 expertise. How do you tailor education to accommodate
13 that?

14 MR. KELLOGG: I think that's one of the driving
15 reasons behind this National Cyber Safety Alliance and
16 Stay Safe Online is that it brought together industry
17 and government to tackle a lot of these issues, some of
18 which were behavioral, but mostly what can we do to
19 collectively reach out and educate small businesses and
20 consumers about what they can do to harden systems.

21 But, for example, on the behavioral side, you
22 have links to a variety of organizations there that
23 focus specifically on this, like the Cyber Safety
24 Citizenship Initiative, Stay Safe Online.com, which is

1 actually a Microsoft initiative. You have a number of
2 other programs that are available on Stay Safe Online
3 that you can link to that cater to a younger group as
4 well as parents and educating them on what they can do
5 to proactively address some of these issues.

6 So I don't want to beat the horse to death, but
7 sometimes there are solutions right in front of us, and
8 it's not all about the technology and the tools. It's
9 also about this is an ongoing continuous process, and
10 having one stop where you can get a lot of this
11 information if you're a consumer or you're a small
12 business or a medium sized business is helpful, and
13 that's one of the driving reasons behind Stay Safe
14 Online and that campaign and why we formed the alliance
15 in the first place.

16 MR. KUO: Earlier this morning we were talking
17 about how consumers don't get enough education about
18 this. Yet at the same time we're saying that 40 percent
19 of people that were surveyed had received viruses and,
20 20 percent of them had evidence of, received it four or
21 more times. That's saying 40 percent is actually
22 getting educated and 20 percent are often getting
23 educated quite often, but we're still in the stage where
24 this education still needs to be tackled by educating

1 the educators. We can't get out to all those people
2 that quickly.

3 . During the Code Red crisis, I did some
4 calculations, and during the crisis period, 60 to 90
5 percent of the servers that were infected at the
6 beginning were no longer infected by the end of another
7 week, so we were getting the message out during a crisis
8 period, and without the pain of crisis, people just
9 don't pay attention, so back to what I was saying.

10 40 percent of the paper are now getting educated
11 because they have firsthand experience so unfortunately
12 they're learning it the hard way, and the rest of the
13 population are either going to learn it the hard way or
14 they're going to wait for somebody close by to suffer
15 before they learn it.

16 But if we can teach enough of the teachers to
17 get out there, we may be able to I guess shorten the
18 number of degrees of separation so that there are other
19 people that feel the pain of the neighbor as it
20 were a pain for themselves.

21 MS. BERGER: In just a minute or two, we're
22 going to be moving to Q&A, but now that we've been
23 discussing the importance of these broadband campaigns
24 and of educating the educators about how to reach people

1 through these more broadband campaigns, I'm wondering if
2 anybody wants to highlight particular things that
3 individual businesses might be doing to reach consumers
4 who use their sites, something like what Tatiana has
5 mentioned about telling a consumer "continue to type the
6 URL" at a time when it might be especially pertinent to
7 the consumer.

8 MR. JORDAN: I have actually a pretty good case
9 study on that, but before I go into that, I want to
10 build on something Jimmy said. We have to think about
11 this in terms of market adoption. You have 60 million
12 households in the United States that have adopted in
13 some form or another of technologies, but that doesn't
14 mean -- of computer technologies. That does not mean
15 they've adopted the same computer technologies, all of
16 them.

17 So you have these waves of adoption that are
18 currently taking place, and some people are up to say
19 like Windows 95 and others are up to 2000 and others are
20 up to NT, so we're dealing with a plethora of adoption
21 sets, and I think that that's one of the reasons why you
22 have to break it down between behaviors versus tools.

23 Because of the fact that the rate of
24 technological change is proceeding like this, I think

1 that you're always going to see a lag in technical
2 adoption or adoption of technological techniques.

3 That being said, segue very badly, this is a \$10
4 million direct sales company in Florida that is putting
5 information about scandals and scans on the back sheet
6 of their -- of just their basic newsletter. What we're
7 seeing is that companies like the National Companies,
8 the National Company are really trying to educate their
9 own consumers because they see it as a unique selling
10 tool for themselves.

11 So we see this ranging from the very small \$10
12 million type company to the hundred million to the
13 billion dollar folks, and again it ranges from folks
14 that care about their consumers to folks that are caring
15 about their employees to folks that are caring about
16 their marketplaces.

17 MS. BERGER: I'm going to allow just one more
18 comment from Tatiana, and the people that have Q&A, you
19 can go ahead and approach the microphone because we're
20 going to move to that immediately afterwards if there
21 are any questions from the audience.

22 MS. GAU: You asked for other examples of ways
23 in which messages are getting across to consumers. I'm
24 going to point to the Code Red example where the

1 national infrastructure protection center of the FBI
2 actually held a press conference. It hit the headlines
3 of all of the major newspapers. It was on the TV. It
4 was on the local news. It was on the national news.

5 It was something that really got the attention
6 by using the mass broadcast media, which as I indicated
7 before, we found that in the survey we did respondents
8 were getting their information from TV still, and that's
9 the average consumer that that's where they're hearing
10 about problems.

11 Incidentally I would like to say that that survey
12 is on the Stay Safe Online.info web site. You can link
13 to it from the web site.

14 MS. FRAKER: Hi. My name is Mary Faker. I'm from
15 Powell Tate, and I have quick questions for Tatiana and
16 I'm sorry, is it Bernhard?

17 MR. MEISTER: Yes.

18 MS. FRAKER: Tatiana, and I apologize I don't
19 have AOL and I also don't have broadband so that may be
20 the cause for my ignorance.

21 My question for Tatiana is someone this morning
22 mentioned that there's some aspect to Instant Messaging
23 that can somehow make the recipient of the Instant
24 Message more vulnerable. Is there anyone in here that

1 can say that better? I'm not sure if it breaches a firewall
2 or what, but apparently there's some --

3 MR. FOX: There's file exchange options in
4 Instant Messaging.

5 MS. FRAKER: Thank you. I was wondering if this
6 is a potential with AOL Instant Messaging and if so, is
7 that one of the sort of warnings or advisories or
8 whatever that you make available?

9 MS. GAU: The file sharing functionality on
10 Instant Messaging is actually something that is
11 optional. It is not automatic. Somebody earlier
12 mentioned the tip of turning things off if you don't use
13 them. That's one approach to it.

14 With AOL's Instant Messaging system, we actually
15 have a series of permission windows that will alert the
16 user as to what exactly is about to happen, that
17 somebody wants to share a file with them or wants to get
18 a file from their computers asking for a file from them
19 where there is no way that that consumer can just by
20 accidentally hitting the return key cause that to
21 happen, that we make sure that they are fully aware with
22 messaging, with pop ups that interrupt their screen, so
23 to speak, to tell them this person is asking to send you
24 a file or is asking for a file from you.

1 So to that extent, we try to prevent the
2 situation from ever getting into a problem situation,
3 but to the extent that the person ignores the messages
4 and just willy nilly agrees to accept files from
5 strangers, they are going to be at risk.

6 MS. FRAKER: Is there some kind of a warning?
7 Is it a yes no thing, or is this some kind of warning,
8 You may not want to do this because?

9 MS. GAU: There is a warning.

10 MS. FRAKER: My question for you, sir, is we've
11 gotten a million calls from people offering us Verizon DSL.
12 Does Verizon DSL have a firewall or at least in the
13 process of becoming a Verizon DSL subscriber, would I be
14 advised of the need for a firewall?

15 MR. MEISTER: That's not my part of Verizon
16 personally, so I won't try to tell what's going on
17 there, but I know for a fact that there are lots of
18 discussions and lots of activities in this arena because
19 we also use this technology extensively. We have many
20 home commuters who take the opportunity to dial from
21 home, and many of those people dial from home using
22 broadband connections.

23 So we as a large corporation are moving actively
24 in this sort of arena to protect our customers, and I

1 would imagine that the Verizon online folks are working
2 to protect the online DSL users as well.

3 MS. LEVIN: Hi. My name is Toby Levin with The
4 Privacy Council, and I have a question regarding the
5 technology skill gap. Consumers have been given the
6 blessing of computers in their home, but with that
7 there's a major technology skills gap unlike the car where
8 consumers can just take drivers ed.

9 They can take classes, learn how to drive a car
10 and they're off. When there are security or issues
11 regarding safety, they pretty much can rely on various
12 sources for information to address those concerns.

13 Well, with regard to computers, here's the
14 technology that is probably at least as sophisticated as
15 automobiles, if not more so, but yet consumers aren't
16 equipped to really handle all the security repairs and
17 safety issues involved. How do you address the fact
18 that -- is this a short-term problem or a long-term
19 problem?

20 Will consumers with the education that you're
21 suggesting that's underway, is that enough to really
22 address the security issues given the sophistication of
23 the tools that they now have at their disposal?

24 MR. JORDAN: I know you're going to hate this as

1 an answer but it depends. I think that right now
2 actually we're in the stage of a thousand flowers are
3 blooming, whether it's in terms of policy, whether it's
4 in terms of threats, whether it's in terms of
5 vulnerabilities, whether it's in terms of different
6 product lines, I think there are a plethora of web sites
7 and available tools that are out there.

8 The problem that you have is that because there
9 is a wide range of tools out there doesn't necessarily
10 mean that there's been a shake out of what the best ones
11 are for the particular groups. I think that a market
12 idea that there may be a market solution for this,
13 whether it's the establishment of businesses that they
14 come and check your security for your home every month
15 or something like that or some kind of outsourced
16 business administrator, things like that will start to
17 evolve.

18 And just as you have your pest control
19 exterminator come once a month, you'll have your virus
20 and online pest control exterminator come once a month.
21 Who knows what the long-term solutions to that will be,
22 but I think that right now we're in the growth stage
23 before kind of the shake out of consolidation.

24 These are not mature industries. We're talking

1 about industries that are what, a decade, two decades,
2 three decades old at the most? This is a process that's
3 still evolving and rapidly.

4 MR. KELLOGG: But, Steve, when you also think
5 about the tools available out there and you look at
6 tools two years ago versus now, the fact is they are a
7 lot easier to use than they were, and they're getting
8 easier to use. The technology is moving very quickly.

9 Always when we talk about this point, I always
10 think about an older family relative of mine who started
11 using a computer several years ago. He is of the
12 greatest generation and so he came into computers late,
13 and then he started using them and get interested and do
14 a lot of things with them.

15 But it took him awhile to understand that with
16 that came responsibilities, and then when he understood
17 that, gee, this is really -- these things are just hard
18 to use, well when he actually started to try to update
19 his system on a monthly basis and then on a weekly
20 basis, he then found out that they weren't so hard to
21 use.

22 So it gets back to what we were talking about,
23 increasing awareness and getting over that barrier, sort
24 of the lack of education out there, whether it's among

1 consumers, small businesses or medium businesses,
2 there's just a lot of fear there, and it's going to take
3 time to overcome that, and it takes a real effort, and
4 that's again what we're trying to do in this industry
5 and what I think we're seeing in government as well in
6 partnering with us.

7 So it's important to remember that this is going
8 to take time, and it's nothing we can immediately
9 overcome.

10 MS. BERGER: On that note, I can take one
11 parting remark from a panelist, and I see two of you
12 leaning forward to grab it. I think I happened to see
13 Tatiana first, and then we'll have to close this
14 panel and move immediately into the next one hour
15 segment. There will be a break after the next one hour
16 segment.

17 Tatiana?

18 MS. GAU: Actually in summarizing your comments,
19 I agree with everything you said, but I think that the
20 consumer is never going to be inclined to learn all the
21 details about what's going on in the computer. It's
22 like in the car. I mean, I know I have an air bag
23 system, but I don't care to know about the technology
24 behind the sensors that's going to set those air bags

1 off.

2 I just want to know those air bags work, and I
3 base my decision on the company from whom I buy the car
4 and the assurances they make because I trust them as a
5 brand and as a company that they'll do the right thing.

6 There is a lot that companies in the Internet
7 space and the technology space right now can and could
8 be doing on the back end to help protect consumers. We
9 do a lot of that, and as I mentioned already, we rely on
10 customers to tell us what problems they're experiencing
11 in order for to us respond to it, but there's more that
12 could be done in that area, and I think that is what is
13 key, combined with education as to really simple, easy
14 to remember tips for the consumer.

15 We can't overload them with heavy technical
16 detail at this point. We've got to take some
17 responsibility through our online industry associations,
18 other kinds of trade associations, partnerships with
19 government and things of that sort to really get the
20 word out.

21 MS. BERGER: I would like to thank each of our
22 panelists for participating this afternoon. Thank you.

23 (Applause.)

24

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1

2

3

4

5 PANEL III: WHAT EXISTING BUSINESS MODELS HELP

6 CONSUMERS MAINTAIN SECURITY?

7 MODERATOR: LAURA BERGER

8 PANEL MEMBERS:

9 SCOTT CHARNEY, Chief Security Officer, Microsoft
10 Corp.

11 STEPHEN COBB, Senior Vice President, Research &
12 Education, ePrivacy Group

13 SIMSON GARFINKEL, Chief Technology Officer,
14 Sandstorm Enterprises

15 JAMES C. PLUMMER, JR., Coordinator, National
16 Consumer Coalition Privacy Group, Consumer Alert.

17 MS. BERGER: We're going to move ahead in just a
18 minute here to begin our next panel.

19 I'm Laura Berger. I'm going to continue as your
20 moderator for the next panel and introduce the
21 panelists. Well, this panel is going to -- in the last
22 panel, we were talking about what consumers' need to
23 know and how to get them to know about it, to educate
24 them, and now we're going to talk about business models

1 that businesses can use to get consumers to start doing
2 them, to get consumers to start using security products
3 and incorporating security into what they do.

4 And immediately to my left we have Scott
5 Charney. He's chief security officer for Microsoft
6 Corporation, and on his left we have Stephen Cobb,
7 senior vice president for research and education for
8 ePrivacy Group.

9 Going down the line again to the left we have
10 Simson Garfinkel, chief technology officer, Sandstorm,
11 and an author of among other things Web Security,
12 Privacy and Commerce and also of Database Nation.

13 And on the far left we have James Plummer,
14 Junior, coordinator of the National Consumer Coalition
15 Privacy Group for Consumer Alert. So I would like to
16 welcome you all, and as with the last panelist, I
17 probably won't have to cut people off as I did on the
18 next panel, but we're going to go with the same format
19 of just discussing with questions what we've been
20 talking about.

21 So just as a segue from the last panel, to start
22 with, what is the role of education in getting consumers
23 to use security products?

24 MR. CHARNEY: I can certainly start. Education

1 is the key. I've been in the security space for 12
2 years. Threats aren't really -- or the risk of having
3 something is very small and at PricewaterhouseCoopers,
4 we talked to enterprise customers or even home users,
5 especially those with broadband because we're seeing
6 broadband home access for the first time, and you say,
7 Look, you have to really be concerned about your
8 security and they go, why.

9 And you can show them specific cases that we've
10 worked over the years of serious hacking. You can show
11 them surveys by the American Society of Industrial
12 Security, the Computer Security Institute.

13 The statistics are there, yet people still
14 continue to say, I think the likelihood of me being
15 attacked is very small, and they'll go somewhere else,
16 and this isn't a real threat, and because of that they
17 don't deploy security.

18 So the first step has to be education. People
19 have to recognize that these threats are real, that
20 there are practical steps they can use to mitigate their
21 risk, and then they have to implement those steps, and I
22 think -- then I'll turn it over to other panelists, but
23 I think part of the problem is that this information
24 technology threat is not very intuitive.

1 Life is all about risk management. You can walk
2 out of this proceeding and get hit by a car and killed.
3 It's unfortunate, but it happens every day to somebody,
4 so you go to the corner, wait until the light is green,
5 and you look both ways before your cross.

6 You exercise risk management, but that's
7 intuitive. When you're talking about technology, it's
8 not intuitive, and therefore far more education is
9 necessary.

10 MR. COBB: I'm going to pick up on the
11 automotive analogy because they seem to have been
12 running as a theme through today, and I was struck by
13 the earlier comment about only one in ten DSL vendors
14 providing a firewall.

15 It was like selling a car without seat belts and
16 airbags, but I think the education analogy is closer to
17 the ad you see for the kid in the car who's going, I
18 don't know how many miles an hour, and he's shifting
19 gears, and you see the tachometer, and this car looks
20 great, and every kid wants to buy one.

21 There's a little message down at the bottom that
22 says, Professional driver on closed circuit, do not
23 attempt, and I think vendors in this space have a
24 problem, a dilemma, if you will, in that we want to say,

1 hey, dude, you're getting a Dell, but we don't
2 necessarily want to say, Hey, dude, you're getting a
3 virus.

4 And you have a dilemma as a vendor, which I
5 sympathize with in terms of pushing forward the
6 technology, and the advantages of the technology, at the
7 same time making people aware of the risks of the
8 technology, and so I agree certainly with Scott that
9 there is this problem of perception of the risk.

10 We were talking about this at lunch, about
11 putting numbers on what it costs you, even as a family
12 to have a virus problem, and I again spent many, many
13 years in the business and numbers upon numbers each
14 year, and we do get better numbers I think now than we
15 used to.

16 But quantifying the risk in terms of numbers may
17 not necessarily be the way to go for consumers. I think
18 if you had video of people stressed out over losing
19 their information that might be close to what I see on
20 the consumer end of things, but certainly a way of
21 getting across to people, I think someone in an earlier
22 panel mentioned the seat belt analogy and the gruesome
23 pictures, possibly the video of the stressed out user
24 who's lost all their information due to a virus, is that

1 analogy, carries that over.

2 But the problem -- and in approaching the panel
3 I was thinking about the question of the business model,
4 I'm not quite sure who is going to pay for the education
5 that's really going to say, well, there are down sides to
6 the technology, so I think that's possibly a role for
7 independent parties. There are industry associations,
8 organizations like TRUSTe who play kind of an
9 intermediate role in the technology to step forward and
10 explain that side of it.

11 I don't necessarily think it's even fair to ask
12 inventors to go too far down the road of saying, Well,
13 what we're selling you is dangerous because if it is
14 used properly, it need not be dangerous.

15 MS. BERGER: Does anybody want to chime in with
16 any examples there might be of businesses educating
17 consumers about risks associated with products? Simson,
18 did you want to speak to that point?

19 MR. GARFINKEL: I'm sorry, I was going to
20 finish.

21 MS. BERGER: Go ahead. I can raise that again.

22 MR. GARFINKEL: Thank you. I wanted to say that
23 throughout all of today, we've had a real "blame the user
24 approach" in this conference, this workshop, and clearly

1 it's the user's fault so they should be blamed, but I'm
2 not sure that that's entirely fair.

3 Earlier the questions like why don't the people
4 selling DSL connections supply a firewall with the
5 modem, and that's a good question but a better one would
6 be, Why don't they program their routers so that firewalls
7 are not needed? Why don't they program their
8 email system so that they're doing virus scanning so
9 virus scanning isn't needed on the desktop?

10 Making a business case for increased security
11 services was mentioned earlier. One problem that we
12 have with the increased security services for the users
13 is that the companies that are trying to make money
14 selling Internet services are systematically sabotaging
15 attempts to have increased security and privacy.

16 You may remember that back in the 90s we had a
17 huge public education campaign about the importance of
18 digital certificates and the little lock at the bottom,
19 but Microsoft and Netscape both refused to modify their
20 browser so that the certificate name, the CN, would be
21 displayed.

22 And now most of the companies that are doing
23 secured web sites don't do their own credit card
24 processing, so the HCPS is going to a third-party.

1 One of the earlier panelists said that a huge
2 problem that we have is web sites going up, looking like
3 they're from IBM but really being from like somebody in
4 Korea. The whole digital certificate infrastructure was
5 supposed to prevent that, but the way that the web has
6 been commercialized has defeated those security
7 measures.

8 So you asked how education and how business
9 models can bring back -- give us better security, and
10 I think that in one part we're blaming the wrong
11 people. I think blaming the user is a lot of fun, but I
12 think that the real business is going to be made off of
13 bringing back the security that we knew how to build in
14 in the beginning and that we haven't built in for
15 reasons of misguided attempts at usability or trying to
16 make quick money off of users instead of doing the hard
17 work and developing these services.

18 MS. BERGER: Okay. So we're starting to frame
19 this discussion a little bit more in -- wherein Simson's
20 remarks are trying to frame it a little bit more or try
21 to keep framing it in terms of business models for doing
22 this, for getting consumers to expect safer products or
23 being able to through your business deliver safer
24 products that consumers will be interested in adopting

1 and will, for example, be willing to pay more.

2 As someone suggested this morning consumers
3 might be willing to pay more for a safer ISP. What are
4 the sort of ways that businesses can bring these
5 products to consumers and consumers will be interested
6 in selecting safer products?

7 MR. PLUMMER: If I could get in the initial
8 questions about education. I think what businesses
9 should look at is why consumers are on the Internet, and
10 consumers are on the Internet for two reasons. One is
11 for convenience, especially for consuming and actually
12 buying products, and to gather more information,
13 information on things that interest them or entertain
14 them, and unfortunately many consumers just aren't that
15 interested or entertained by treatises on 32 bit
16 encryption security.

17 So you have to try to get -- take advantage of
18 the consumers' need for convenience but yet acknowledge
19 their reluctance to get deep into technical details and
20 add both of those in you're thinking when you're trying
21 to get consumers to harness security and more security
22 education.

23 For instance, the Dell came up earlier. I just
24 got a new Dell laptop and that came with demo-ware of

1 Norton anti-virus, and that was free to me, and any
2 consumer who has not had an anti-virus program before,
3 they get this free run for 90 days. They will, as has
4 been mentioned before, get an education on exactly how
5 many viruses might come into their email, provided the
6 number.

7 So I think that one way is to do it is if you're
8 selling security products is to just show -- show what
9 your product can do, and you can do that for free by
10 demonstration ware or take another model, for instance,
11 some alarm firewalls and probably other firewalls have
12 a home use option that it's free, and that way the
13 consumer gets free use of the security software, but if
14 he's the kind of person that makes decisions or is
15 influenced on the decisions for his business which is
16 what they're hoping by giving away the free software,
17 you have to take that knowledge to the office and maybe
18 use that same product at work.

19 So that's just a couple initial ideas on
20 education.

21 MS. BERGER: Okay. Scott wants to follow up on
22 that.

23 MR. CHARNEY: Well, yeah, I think as a practical
24 matter, there are a lot of people who go out and shop

1 for other things like cars that may not know what a fuel
2 injected engine is or may not understand automobile
3 engineering but will buy a Volvo because they perceive
4 it safe based on a safety campaign and maybe even
5 independent tests.

6 So I think as a practical matter for vendors of
7 products, the key is once consumers are educated that
8 they actually do need to take security seriously and
9 that they should be investing in security products, how
10 are they going to go out and buy those products?

11 Well, they're going to do it like they other do
12 other things. They're going to look at brand and
13 business integrity, and certain brands have a certain
14 level of trust. They're going to look at ease of use of
15 the product and how easy it is to install and manage.

16 And they're going to look at independent
17 testing, to the extent groups test different products
18 and write magazine articles or do some consumer reports
19 on security products, they're going to go and look at
20 those and say, Which ones have the red circles, which
21 ones have the black circles for ease of use, the number
22 of threats that are covered, how easy they are to
23 maintain and the like.

24 And I think we sometimes got bogged in saying

1 consumers have to understand all the nuances of the
2 technology but I'm not quite sure that's true. I'm not
3 sure they understand all the nuances of how automobiles
4 work, but there are still metrics that consumers use when
5 they go to the market, and I think we should look at
6 that in this space as well.

7 MS. BERGER: Okay. Simson?

8 MR. GARFINKEL: One of the problems is there
9 isn't a good alignment between where the money is being
10 made and where the security is. The people who are
11 selling the most insecure products are making the most
12 amount of money in this consumer space.

13 The Microsoft products are the least secure, and
14 people are making the most money selling them. The
15 Apple products are more secure, and it's a much smaller
16 market segment, and the Unix products, Linux, the free
17 software ones are even more secure, and there's even
18 less money being made there.

19 So there's a whole problem trying to use the
20 market, except for like the tort system, to reform us.
21 It's much closer to how do you regulate the tobacco
22 industry than how do you regulate the car industry.

23 MS. BERGER: There's going to be a separate
24 panel on legal standards and standards for regulation,

1 so just if we can stay focused on the business models
2 for this panel.

3 MR. COBB: That's the difference between Scott
4 and Simson. I mean, I hear what Simson's saying. I
5 think -- I mentioned for somebody who spent 15 years
6 looking at all of the things that can go wrong with
7 these things, I'm actually quite optimistic because what
8 I've seen over the years in security is that it's all
9 about timing.

10 And you could have had a great idea for a
11 security product five years ago, and nobody would have
12 bought it because there wasn't sufficient critical mass
13 in terms of understanding what the problem was, and
14 although we've been really sort of drowning in the woes
15 and the problems which are certainly real at the moment,
16 I do sense a rising tide of understanding in the
17 marketplace amongst the consumers.

18 And I do think the pressure that really led for
19 say, for example, Volvo to succeed with the idea of a
20 safer car, I think that may well arise, and that market
21 pressure I think will have an effect, and I think we
22 would have to acknowledge that Bill Gates did send this
23 memo around at Microsoft saying, We have to focus more
24 on security than features, and I don't think he did that

1 out of a sense of patriotism.

2 I think there's clearly a business model in
3 which or an economical model in which people's
4 dissatisfaction with things reaches the point where they
5 stop spending money, and I think a smart business model
6 for some company might be to fund an independent
7 third-party to put out ads about all the terrible things
8 that can happen to your computers and some of the steps
9 you can take to solve them while at the same time
10 marketing a product which they stress the security of.

11 Not to be cynical about it, but I think, yeah,
12 one way or another there's going to be an increased
13 consumer pressure for better, safer products in the
14 space and companies are going to respond. I do see waiting
15 in the wings legislators and regulators that are
16 concerned that the consumer is perhaps getting the raw
17 deal.

18 MS. BERGER: Scott?

19 MR. CHARNEY: I think it's important to note two
20 things. People don't buy products just for any one
21 feature, not just for security, so even people who buy
22 cars who might want a safe car wouldn't buy a car that
23 has a great safety rating but breaks down every two
24 months, so consumers are actually more complex than

1 that.

2 But I would say we see a synergy of two
3 different things happening, that I completely agree that
4 I'm very optimistic about the future and the synergy is
5 this: On the one hand, you finally have markets
6 demanding security, and if the Justice Department kept
7 going out and telling people that cyber crime was a huge
8 problem, they kept saying, no. Now you don't hear that
9 anymore.

10 And to the extent consumers and enterprises
11 demands security, then the market builds security, but
12 the second thing which is also very real is the threat
13 model is changing. If on September 10 you said to me,
14 What are the odds of four planes being high-jacked,
15 three of them hitting buildings and two World Trade
16 Centers collapsing, I would say the threat of that is
17 almost zero.

18 And then this happened, and as a result of that
19 and Code Red and NIMDA and a bunch of stuff, people are
20 reassessing the threat model. We're throwing out what
21 we assumed were givens and we're reassessing, and the
22 result of that is a lot of companies -- I mean, there's
23 no question that Microsoft sees a market in security.

24 But Microsoft has actually been working on

1 critical infrastructure protection systems for quite a
2 long time, and we are now escalating that a great deal,
3 and let's face it, I'm a cost center to the company, but
4 we're doing a lot of stuff, and a part of it is not just
5 markets but public and social responsibility.

6 We have to protect these infrastructures or
7 we're not going to have the society we aspire to and
8 you're not going to protect these infrastructures without
9 insecurity, so we have to get it right for a host of
10 reasons, and that now a combination of markets, threat
11 models, critical infrastructure protection, there's a
12 lot of reasons to think that everyone at every level is
13 going to take this seriously, and we are going to start
14 moving much faster down a path in the right direction.

15 MS. BERGER: Yes?

16 MR. PLUMMER: If I can follow up on a couple
17 things that people said. I think a lot of things that
18 everyone said make sense when seen together. The
19 importance of brand names was mentioned, and that's very
20 true, and Microsoft has indeed got a reputation for
21 security over the last three years, which is why Bill
22 Gates is having this big push to increase security.

23 So Simson definitely had a point there, and it
24 is true that consumers are complex, not just looking for

1 security but for other features, and part of the reason
2 why Microsoft has been more vulnerable is that's what
3 almost everyone uses so that's what most of the viruses
4 are written for.

5 They're written -- I have Windows myself but I
6 don't use the Outlook email system. I use Eudora
7 because many of the viruses are written -- they'll go
8 off easier if you have Outlook.

9 So that's another thing that as far as brand
10 names go, first of all, it's a good idea for consumers
11 to diversify where possible on their home computers, and
12 if everything is linked and one thing goes down, then it
13 all goes down, but companies like Qualcomm who have that
14 advantage, they should advertise it.

15 If companies think their product is more secure
16 and they honestly believe that, they should advertise
17 that. Earthlink should advertise the fact that they're
18 a lot less likely than say AOL to just turn over all
19 your information to the first guy with a badge that
20 shows up at your door, so these are all very important
21 things to talk about.

22 MS. BERGER: I want to turn the discussion a
23 little bit. We've been focusing on security that's
24 embedded in software and saying consumers don't just buy

1 a product for security it can offer them.

2 What about business models where you actually
3 just sell supplemental security products, are those an
4 advantage for consumers?

5 Simson?

6 MR. GARFINKEL: I have a real problem where
7 you're selling a product, and then there's an additional
8 product that you need to buy to make it secure.

9 MS. BERGER: Assume there's a separate vendor.

10 MR. GARFINKEL: If it's the same vendor or
11 separate vendor, I think that's anti-consumer, and I
12 think that products should be delivered that are
13 secure. I also think that in the field of computer
14 security, it's very difficult to advertise that one
15 company is more secure than another, and I didn't mean
16 to attack Microsoft earlier. I only meant to attack
17 their software.

18 The problem is that all the software that's out
19 there has security vulnerabilities, and if you advertise
20 that your product is more secure and then a
21 vulnerability is found as invariably an -- as invariably
22 the vulnerability will be found, you look like you are a
23 liar or a cheat, and this is really difficult for the
24 companies.

1 MR. COBB: But I think -- I don't know that it's
2 necessarily reasonable to expect every threat to be
3 anticipated by a vendor. If you look at the development
4 of say anti-virus software, neither the hardware
5 companies nor the application companies or the operating
6 system companies sold anti-virus software in the early
7 days because there were hardly any viruses.

8 Then as viruses became more prevalent, people
9 gave out the anti-viruses to fight them, and some of
10 those companies are still around selling that as an
11 add-on. In fact Microsoft introduced a form of
12 anti-virus in DOS 6.something, and it didn't stay in
13 there very long.

14 So I would say that there is a valid market for
15 an add-on product. It is addressing a threat that
16 hasn't yet been internalized by the software, but on the
17 other hand, I would agree that there is a base level of
18 security that consumers should be able to expect from
19 their hardware, software and applications that right now
20 we're not seeing.

21 MR. GARFINKEL: See, what I would like to see
22 instead is more emphasis on services. Now, the
23 anti-virus people are actually doing that, and they have
24 largely migrated what they offer from being a program

1 that you buy to an update service, and I would like to
2 see more kinds of services like that. The single biggest
3 problem that consumers have with their computers is that
4 they do not back them up, and there should be better
5 emphasis on back up services and back up products like
6 that.

7 A second huge problem is data sanitization. A
8 few years ago I bought some used computers, and let me
9 tell you what I found. One of them had been used by a
10 law firm, and there was a lot of confidential client
11 attorney privileged information on it, and another had
12 been used by an organization that delivered mental
13 health services, and there was a list of names and
14 diagnoses.

15 Those machines when they were sold to me, they
16 should have been sanitized. There is one or two
17 companies that actually are doing this for a business,
18 but there is very, very few of them, and there's very
19 little information out there for consumers on how to
20 properly dispose of a computer. There's a lot of
21 erroneous information such as you can't ever erase all
22 the information, which is just not true.

23 MS. BERGER: So what's a -- framing this again
24 in terms of business models, how would a business be

1 able to encourage a consumer to take steps when
2 disposing of a computer to make sure that it's
3 sanitized?

4 MR. CHARNEY: Part of what I'm hearing, it comes
5 back to your first question about an education problem.
6 There's been file wiping utilities on the market for a
7 long time, and I agree that people need to use them, and
8 there have been well reported cases of companies sending
9 machines to surplus or put on the secondary market that
10 haven't been appropriately wiped.

11 I think Washington Mutual was one of them, and
12 there have been others, but the utilities exist to do
13 that, and it's interesting that in my days at
14 PricewaterhouseCoopers when I was doing security
15 consulting how we kind of assume that at the enterprise
16 level, the IT staff is just incredibly competent. They
17 can get everything done, and the reality is that's
18 just not true.

19 This technology exploded far faster than our
20 educational institutions could train people to do this
21 technology, and I'll give you a real life case in
22 point. In 1991 when I became chief of the computer
23 crime unit, I went to Johns Hopkins with a colleague to
24 take a course on networking in computer security because

1 I now had this new tasking, and he and I are in this
2 classroom which was taught by an instructor from the
3 Defense Department, and we were there with 12 women, all
4 roughly 22 to 24.

5 And the instructor wanted to go around and say
6 why were you taking this course, and my colleague and I
7 explained that we were now prosecuting this stuff and
8 needed to get a handle on what we were doing, and as
9 they went to everyone else it was, I was a secretary in
10 the medical department, I was really good formatting
11 documents, they've now told me I'm the LAN
12 administrator.

13 Each one came from a different division at Johns
14 Hopkins, so one of the problems is sometimes the tools
15 are there, but the people are not appropriately trained
16 to handle this, and of course it gets even more
17 difficult at the consumer level.

18 We don't have a unified user base. It's not
19 monolithic, so when my mom went on email that was
20 great. When she started thinking about broadband and I
21 tried to explain firewalls, the conversation went
22 downhill pretty fast, and so even at the enterprise
23 level very often the people -- the tools are out there
24 in the marketplace but the business processes are not in

1 place to do it right.

2 People aren't educated enough to do it right and
3 they don't audit the processes even when they're
4 supposed to be doing it to make sure it's actually being
5 done right. So there's a lot of things at the
6 enterprise level that businesses have to do.

7 On the consumer level my view is that vendors
8 and service providers have to do more because I don't
9 think -- we can educate consumers on the threats. They
10 can go into the marketplace, but this technology, we do
11 not yet have what I call security usability. Security
12 is just not that simple to use yet. We have to get it
13 there.

14 You know, you buy a hair dryer. In the old days
15 you bought it, you look for that little UL label on the
16 cord because you didn't want to electrocute yourself,
17 and that UL label said it was safe, and you went home
18 and plugged it in the wall. Now you go out, you buy a
19 hair dryer, you plug it in the wall, you don't think
20 about it.

21 We all know electricity is safe. We all know
22 hair dryers are safe. Nobody thinks about it. That's
23 where we need to be with computer technology. We are
24 not there yet. We will not be there for some time, but

1 we have to work in that direction.

2 MS. BERGER: We are going to move to Q&A in just
3 a minute here, but I wanted to talk about just one more
4 type of business model or product to get consumers to
5 secure their own computers. We have talked a little bit
6 about supplemental security products and what role they
7 might play and in improving security and security that's
8 included in software.

9 What about transaction based security products,
10 what kind of role do those have in getting consumers to
11 set up their computer?

12 MR. COBB: You mean securing transaction as they
13 occur?

14 MS. BERGER: That consumers might conduct, yes.

15 MR. COBB: I think if you're talking about
16 increasing the level of security, some of the speakers
17 this morning talked about two factor and three factor
18 authentication, moving to that level.

19 I think it's interesting to see what's happened
20 in the marketplace where we've had initiatives like the
21 blue card from American Express which is a smart chip
22 which as far as I know isn't actually being used as a
23 smart card at this point, and I have a sympathy for
24 vendors that have pushed them.

1 I had an account with the Royal Bank of Scotland
2 which is one of the first to push out digital
3 certificates to use. This was a number of years ago.
4 Unfortunately, it was very, very complicated, and if
5 your computer sort of died for some reason, then it was
6 a whole series of phone calls to get it back.

7 And yet you had to admire them for going that
8 extra mile. I think it's a difficult one because if
9 you're going to push security to the point where it
10 involves another layer of inconvenience and it's
11 conceived as that by the consumer, then you've got
12 resistance. I think possibly industry wide initiatives
13 to kind of raise the threshold might be in order.

14 MS. BERGER: So there's some tension there for
15 consumers because businesses have some hesitation to
16 implement the extra steps, but at the same time you want
17 consumers to have an incentive to look for those kind of
18 guarantees.

19 MR. GARFINKEL: The real problem is that we've
20 traditionally framed security and ease of use in
21 opposition to each other, and the very best security is
22 security that actually improves ease of use rather than
23 makes it harder. There are ways to do this in the
24 electronic transaction era.

1 For instance, your ISP could offer some sort of
2 enhanced security service that works with the merchant
3 that you're buying from and like feeds off quality ID or
4 feeds off their radius server or something, but that's
5 really hard to get working, and nobody's even thinking
6 about that right now.

7 I do feel that there is a future out there that
8 Scott's talking about where the systems are more secure
9 and where they're easier to use and people are making
10 money off of this and nobody can do any bad things any
11 more, but I think it's going to be much harder to get
12 there.

13 In the meantime I think that we need to hold the
14 people providing the software more responsible. For
15 instance, there have been file wiping utilities, but I
16 should be able to tell the operating system that I'm
17 selling the machine now, please self destruct and it
18 doesn't have any system for doing that.

19 MS. BERGER: Okay. I'm going to have Scott comment
20 on my question, I think he was ready to, and then we
21 have a line of questioners waiting.

22 MR. CHARNEY: I think to some extent it depends
23 on the transparency of the user. You can compare, for
24 example, SSL to protect credit card numbers in transit,

1 and there has yet to be a documented case that I know of
2 where a credit card has been stolen in transmission
3 because of SSL, the consumer has to do nothing at all
4 compared to the AMEX blue card where I talked to AMEX
5 years ago and they said, Well, the problem is if you get
6 the AMEX blue card, you can call us up and we will send
7 you a free credit card reader, and then we get calls
8 from consumers saying "it says plug into parallel port,
9 what's a parallel port."

10 These are the same consumers who when CDs came
11 out they called the vendors up because they couldn't get
12 the cup holder to retract, so a lot of it depends on the
13 way in which this stuff is implemented and to what
14 extent consumers can use it easily or specifically
15 without even thinking about it like SSL or to what
16 extent do consumers have some role to play in
17 implementing the technology.

18 And if it's a technology that needs to be
19 implemented like two factor authentication, there's a
20 big difference between building it into the keyboard, a
21 card slot, and giving them a third piece of hardware
22 which has to come out of a box, be connected or driver
23 installed.

24 This is not the same thing so we have to focus

1 on making security usable.

2 MS. BERGER: Thank you very much. Questions?

3 UNIDENTIFIED SPEAKER: In terms of speaking of
4 business models, as a consumer. I have a problem with
5 business models. Everyone has focused on a lot on
6 Microsoft, not to beat up on your company too much, but
7 in the bundling of the services, I loaded a firewall
8 from a completely or at least I think it was a
9 completely independent service provider.

10 And one of the things I was disturbed about was
11 not only how many times my computer -- people sought to
12 access my computers but how many times Microsoft XP
13 products would automatically access the Internet to
14 report on God knows about my computer from jukebox to
15 you keep going down the list of the products that I have
16 to keep having to say no, no, no, no.

17 And I wanted to see if the panelists could
18 comment on kind of the conflict of interest that can
19 exist between companies that are configuring their
20 computers to report back on what the user is doing and
21 their providing a firewall to prevent access to the
22 consumer's computer.

23 MR. PLUMMER: If I can say, that kind of goes
24 back to the thing I said earlier about trying to

1 diversify and not put all your eggs in one basket. As a
2 consumer I have a non Microsoft firewall and it's
3 already telling me about my Windows media player and
4 other things that are trying to tell Microsoft
5 something, and I always hit no.

6 So the consumer should definitely be aware if
7 they're getting everything from one place to know what
8 they're doing. I think Simson was advocating earlier
9 that broadband ISPs should provide more security
10 features. That might work for some people, but I think
11 for more sophisticated users, they don't necessarily
12 want that.

13 They want to have -- they don't want the ISP.
14 For one thing it can be inconvenient when it's running
15 everyone's mail through three different filters, but I
16 think kind of dividing what you're using among --
17 diversify is my point.

18 MR. GARFINKEL: I think it's important to pick
19 the right battles, and one of the problems with these
20 firewall home products is they cry wolf because they
21 want people to think they're doing a very good job. All
22 the times that Microsoft products check for feature
23 updates are treated like attacks, and in fact you want the
24 Microsoft products to check for updates because

1 frequently those updates are to deal with security
2 problems.

3 And Microsoft is doing the right thing by having
4 its products checked for updates' use, so it's important
5 -- there is so much misinformation out there that
6 I'm very troubled about.

7 MR. COBB: I let my machine talk about Microsoft
8 in the XP instance because quite frankly I don't think
9 of them as the evil empire, and I think it's a question of
10 trust, and I think that that's probably one of the key
11 elements to building the new economy is the aspect of
12 trust.

13 I think if I trust that they're doing this for
14 legitimate reasons, and I really don't think they're
15 scanning my hard drive for credit card numbers because
16 last I heard they had 40 billion in cash on hand. But as
17 Simson says, it's a question of education, and this is
18 one of the things we're going to have to watch as we
19 move down that road in consumer education.

20 And one of the things my CTO was pointing
21 out to me before I came down here was that the
22 traditional model in security back in the corporate days
23 often as far as selling was fear, insecurity and doubt.
24 You tried to scare up business, and I wouldn't want us

1 to go down that road in terms of over selling the
2 product to consumers.

3 It's a question of making them aware of what are
4 legitimate issues and helping them distinguish between
5 something that shouldn't be coming out of your computer
6 and something which is legitimate.

7 MS. BERGER: Next question.

8 MR. KRAUTHAMER: My name is Michael Krauthamer,
9 and my question is with regard to transactions and the
10 potential use of biometrics for authentication. If a
11 credit card number which is currently stored on file
12 for the purpose of comparing with the number that the
13 user submits to make sure it's legitimate, what happens
14 when or is there a problem with biometric information
15 being stored on a server for use of comparison with what
16 the user submits?

17 MR. COBB: If I could leap right in on that
18 one.

19 MR. GARFINKEL: Are you going to raise up your
20 credit card with a biometric on it?

21 MR. COBB: No, that's a picture on my credit
22 card which I thought was cheap, free, simple, easy
23 working for them, works for me. I didn't have to have
24 this on my credit card. They took the picture at the

1 bank, put it on there, and when the Royal Bank of Scotland put pictures
2 on their credit card, fraud dropped 70 percent.

3 There wasn't any need for Bank of Scotland to
4 store the pictures on a server somewhere, and I do want
5 to make the point on biometrics that it isn't necessary
6 for a central server to store stuff in order for
7 biometrics to work. I could have my fingerprints stored
8 on there, and nobody else would have it. You would just
9 check that it hadn't been changed since it was put on
10 the card.

11 And I would really like to get out the message
12 that biometrics isn't necessarily a big brother
13 assembling all this personal data about it. For
14 example, fingerprint biometrics is not the same thing as
15 the FBI stores when it takes your fingerprints, so again
16 it's a question of education.

17 I think there's been a real problem selling the
18 public on biometrics because this specter of having
19 your identity stolen even more arises. If it's done
20 properly it doesn't have to be a threat.

21 MR. GARFINKEL: The other thing about biometrics
22 is that they are, maybe people do -- every biometric
23 system has a back door. They all fail. They're all
24 probabilistic systems that tell you how close the match

1 is, and the company then is using a test to make a
2 decision about what sort of thresholds or tolerances
3 they want to accept or not accept.

4 So we see a lot of -- the other thing about
5 biometrics is that they're not democratic. Some people
6 will not print with the system. Some people, the live
7 scan fingerprint readers just don't work or the iris
8 scan readers just don't work.

9 So when we deploy these biometrics systems, we
10 have to be sure they're backups or ways of doing the
11 transaction without the biometric. There is so little
12 understanding about the use of biometrics, even among
13 biometric practitioners out there and there are so many
14 people trying to make money selling their particular
15 biometric system, I'm very hesitant to see something
16 deployed for 300 million people.

17 MR. PLUMMER: Just to follow up, Simson is right
18 about the back door vulnerability. All these systems
19 are vulnerable. I do think at least for the foreseeable
20 future, the security responsibilities on the -- it's the
21 onus of the vendor really, not the guy sitting at home
22 trying to buy something.

23 The SSL system seems reasonably secure with
24 credit card numbers and transmissions. I read a report

1 this morning that fingerprints are basically easier to
2 crack than good user names or passwords, and I don't
3 think most consumers are going to be happy about getting
4 their eye scanned to buy a book off of Amazon. I think
5 it seems quite ridiculous.

6 MS. CLAY: Hi, Alicia Clay from NIST. I have
7 just a quick comment about biometrics going to the last
8 question. One of the things I think that we need to be
9 aware of is that outside of the computer security world,
10 people are starting to use biometrics in places that are
11 completely unnecessary. I should not have to give up my
12 fingerprints or to cash a check or to rent a U-Haul
13 truck, so --

14 MR. GARFINKEL: That's to protect your bank and
15 to protect U-Haul.

16 MS. CLAY: So I realize that if I don't return
17 that truck, they can dust the entire world for my
18 fingerprints and try to track me down.

19 MR. GARFINKEL: We want to prove it was you when
20 you don't return the truck.

21 MS. CLAY: Not that they have my fingerprints
22 already, so that they still can tie that thumb print to
23 Alicia.

24 MR. CHARNEY: You need to be careful too because

1 a lot of these technologies, it's not capturing the
2 actual print. It does a mathematical -- it's not like
3 leaving a print on a table, right. It's a little bit
4 different, so depending on the implementation, your
5 print may not be nowhere at all.

6 In the example you gave where you compare it to
7 a credit card for example, the print's not in a
8 centralized database. It's compared locally for you, no
9 one else has it so we have to be careful of that too.
10 We make sure we understand how the technologies work of
11 course.

12 MR. GARFINKEL: What the banks are doing though
13 which I kind of liked was when somebody went to cash the
14 check who didn't have an account at the bank, they put
15 the person's fingerprint on the back of the check
16 itself. That was like with ink, and then if there
17 actually was fraud, if I say I didn't write a check to
18 that person, my checking account was stolen, then they
19 have the fingerprint, the video surveillance and the
20 next time that person comes in with the stolen checkbook
21 they can nab them.

22 If you actually put an ink print on the U-Haul
23 contract and then the truck is not returned and they
24 call you up and they say, Someone using your name rented

1 a truck and never came in, then you can give your thumb
2 print and show that it's a different thumb print, so
3 it's to protect you.

4 MS. CLAY: I want to talk to you more about that
5 off the record.

6 MR. PLUMMER: I wasn't aware U-Haul started
7 requiring fingerprints.

8 MS. CLAY: In certain neighborhoods.

9 MR. PLUMMER: The ultimate thing I can say
10 consumers can do is go to Ryder trucks, just go with
11 your money.

12 MS. CLAY: That's what I did but my actual
13 question I have for Scott really. Scott, one of the
14 things you mentioned was it would be good to have a UL
15 label for secure computer use. That's something that we
16 should be working towards.

17 MR. CHARNEY: I did not say that. I said that
18 in the early days for consumers when they were trying --
19 we were trying to get them to use new products, right,
20 we had the UL label on electric cords to tell them it
21 was safe.

22 Whether in this environment, I mean, there are a
23 lot of independent entities that can assess computers
24 and computer products and all that, so I'm not

1 suggesting it would be one centralized thing, but I
2 think consumers do look for independent evaluation of
3 products as part of their purchase of choice, and I
4 think that's healthy.

5 MR. GARFINKEL: We did the UL label, we did the
6 orange book. You can come and buy an A-1 computer to
7 surf the Internet with, and the problem with that is
8 that the very secure systems are extraordinarily
9 expensive to produce and they're not very functional,
10 and you can't load new software on them.

11 So we could build -- the 30 of us in this room,
12 we could build a consumer computer that would be
13 absolutely secure, that would do the email and do the
14 web and would never be able to take a new virus but they
15 couldn't load any new software on to it, and that's the
16 computer that's going to be sold in five to ten years
17 once we have the feature set nailed down.

18 MS. BERGER: I think we have time for just one
19 more question.

20 MS. FISHER: My name is Vicky Fisher, and I'm
21 going to go back to the car analogy because I work for a
22 car company, but when we're evaluating one car against
23 another, we have a certain set of standards we use, how
24 fast does it go from zero to 60, what kind of miles per

1 gallon does it get, and that gives us the criteria that
2 we say, well, gas mileage is very important to me, so
3 this car is going to meet my needs better.

4 Do we have anything like that that can tell us
5 about what kind of firewall protection we're going to
6 want for my life-style? Do we have any kind of
7 standards that we can agree on so we can rate things
8 against each other?

9 MR. COBB: I think if you look at a slightly
10 more specialized computer press going beyond PC Magazine
11 to something like Secure Computing or Information
12 Security Magazine, there are product reviews and testing
13 is done. I wanted to make the point on, for example,
14 anti-virus software, what used to be the NCSA which I
15 have to say at one point I used to work for used to test
16 and ICA still tests anti-virus to a standard that's a
17 published standard.

18 And I think when they introduced that, that
19 certainly made a big difference to the market. I can
20 remember it was a big instance where IBM started
21 insisting that vendors be certified to that standard.

22 It's a little more difficult, I was involved in
23 the formation of something called the Firewall Product
24 Vendors Consortium, and Marcus Raynum, one of the early

1 firewall pioneers, did draw up a standard language for
2 describing firewalls.

3 That got very, very complicated actually but I
4 think there are publications out there that are testing
5 products and giving you a product with ratings and so on
6 and helping consumers judge, Is this the right level for
7 me, do I need a \$2000 box or a \$50 Zone Alarm license.

8 It's not standardized though to the level that
9 cars are, and that's never going to be the case, that
10 it's just a much more than a vehicle.

11 MS. BERGER: I would like to thank each of our
12 panelists in afternoon, and we'll begin the next panel
13 at about five after three.

14 (Applause.)

15 (Break in the proceedings.)

16

17

18 PANEL IV: WHAT STEPS CAN BUSINESSES THAT MAINTAIN
19 CONSUMER INFORMATION TAKE TO IMPROVE THEIR OWN SECURITY?

20

21 MODERATOR: ALICIA CLAY, NIST

22

23 PANELISTS:

24 MARTIN E. ABRAMS, Hunton & Williams

1 LYNN GOODENDORF, Six Continents Hotels
2 FRANKLIN G. REEDER, Center for Internet Security
3 VINCE SOLLITTO, PayPal, Inc.
4 VIC WINKLER, Sun Microsystems, Inc.
5 MARC ZWILLINGER, Kirkland & Ellis

6
7 MR. EICHORN: Hello, everyone. Our last panel
8 today will be moderated by Alicia Clay of the computer
9 security division at NIST, the National Institute of
10 Standards and Technology. She's on the U.S. delegation
11 to the ISO/ISC subcommittees responsible for developing
12 international standards on information security, and one
13 of her roles at NIST is to handle regional workshops
14 around the country, especially for small businesses
15 about security and security awareness, so Alicia?

16 MS. CLAY: Thanks, Mark. Good afternoon. I was
17 very excited when Mark asked me about facilitating this
18 panel discussion because it does fit very closely with
19 what I'm doing at NIST. Basically we are reaching out
20 to small business owners, trying to teach them about
21 information security.

22 As many of you probably know, the computer
23 security division at NIST puts out a host of documents
24 each year on information security, and about three years

1 ago we decided to see what could we do to help use some
2 of that to help strengthen the information systems of
3 small business, so that's what we're doing with this
4 outreach program.

5 And we're doing that in cosponsorship with the
6 Small Business Administration and with the National
7 Infrastructure Protection Center, but in any case,
8 coming here today gives me a great opportunity to be on
9 the question asking end, so I get a chance to play
10 devil's advocate, and I'm totally excited about that.

11 Now, by way of introduction, I'm going to give
12 just sort of a one or two liner on each of the panelists
13 here. You have their bios, I believe, in your packets,
14 and we'll give each of them an opportunity to give us
15 about five minutes worth of theirs view on security for
16 business systems that are holding consumer information.

17 So first we have Marty Abrams. Marty leads the
18 center for information policy leadership at Hunton &
19 Williams. He is a senior policy advisor to the firm's
20 privacy and information management practice.

21 Marty?

22 MR. ABRAMS: Super. Thank you very much. I
23 should give a disclosure that even though I'm with a law
24 firm, I'm an anthropologist and not a lawyer. I have

1 spent 23 years doing consumer policy, probably the last
2 13 or 14 doing information policy, most of that in the
3 world of privacy, and I have long been interested in the
4 interaction between security and privacy.

5 And when I was with TRW back in the days when
6 they had a big information business, we used to talk a
7 lot with the folks in the information security side of
8 the shop, and those are the folks who do information
9 security for the government and big large organizations,
10 and we talked about the language and the objectives.

11 And one of the things that became crystal clear
12 is that security is typically focused inward while the
13 work we did on privacy was focused outward, that
14 security was based on this concept of protecting assets
15 of securing the organization, and in the world that I
16 now work in, we're talking about pushing and helping
17 consumers to serve themselves more than we serve them.

18 So I go and book my own airplane reservations at
19 American Airlines. I book my own hotel reservations. I
20 deal with all sorts of issues today over the Internet
21 that I used to deal with people who would deal with
22 that, so the whole question of consumer facing security
23 has become a lot more important both to the organization
24 and the business as well as to the consumer.

1 And one of the reasons that we migrate to
2 serving ourselves rather than letting individuals serve
3 us is because of the convenience, and convenience is the
4 driver of the marketplace as we have seen it change over
5 the last 30 years.

6 I often joke about the first time I applied for
7 credit back in 1972. It took me three days to be turned
8 down. Today we would not tolerate waiting three days to
9 be turned down. Today we would like to be turned down
10 in five minutes at the most, and we'll walk away from a
11 vendor who doesn't allow us to do it.

12 So that when question think about the risks to
13 us as consumers it's increasingly that in these
14 interactions there's not just risk to the organization,
15 but there's risk to us as well.

16 Very high quality consumer research that's
17 really been unpublished said that there are three
18 drivers of consumer angst, and the first is I want to be
19 secure and I don't feel that way, and it had nothing to
20 do with any of the things that we were talking about
21 this morning.

22 It was talking about the whole world of identity
23 theft and the driver of the consumer angst as it relates
24 to security is ID theft. The issues that we're talking

1 about this morning are very far from where the
2 consumer's mind is at, but what is real clear is that if
3 we're going to revolutionize the way we interact with
4 consumers so that the networks and infrastructures are
5 more secure, it's got to be done in a way that does not
6 interfere with convenience and is easy to use,
7 incredibly easy to use.

8 It's got to be something that doesn't require an
9 interaction on the part of the individual but rather it
10 is like a tool that is an intuitive tool.

11 If we ask the consumer to act on their own
12 behalf, both to keep themselves more secure and to make
13 the network more secure, we will probably not succeed in
14 doing that. A great example is my wife, and this is a
15 privacy example, she is very privacy sensitive. She
16 tells me that all the time.

17 And so I took our home computer and it's XP and I
18 ratcheted up the whole question of the privacy setting,
19 and two days later my wife, who is very competent and
20 could do these things herself, said, You've got to get
21 on the computer and change whatever it is that you
22 changed and change it back. She says, I can't live with
23 this constant interaction with the computer, clicking
24 through and clicking through. The security devices that

1 we have to come up with have to be easy to use.

2 I think it was very telling on the part of Dick
3 Clarke this morning when he was saying that security in
4 the Defense Department is now a matter of putting a
5 token into a machine, and that same token is the token
6 that opens the door of the building, lets you get in to
7 works. The computer can't work without that type of
8 security.

9 It's easy to use. We're asking the Defense
10 Department people to use something that is easy to use.
11 If we're going to make security work for us and if we
12 have a challenge in protecting the network and we have a
13 challenge in terms of protecting the interaction between
14 the consumer and business, whatever devices we have to
15 do have to be from thinking outside the box to reinvent
16 the way we think about security.

17 It can't be focused on our own assets. It's got
18 to be focused on the needs and the habits and the
19 liveability of the consumer.

20 Thank you.

21 MS. CLAY: Thanks, Marty. Next we have Lynn
22 Goodendorf. Lynn has 26 years of experience in the
23 technology profession with expertise in
24 telecommunications and data networks. Ms. Goodendorf

1 assumed executive leadership of information security at
2 Six Continents Hotels in 1999 and recently added
3 responsibility for data privacy to her role.

4 Lynn is actually unique on our panel here in
5 that she is completely on the user end of security and
6 privacy products and services.

7 MS. GOODENDORF: Thanks, Alicia. I don't know
8 if Six Continents Hotels is a familiar name to everyone
9 because we changed our name about a year ago, and we own
10 and manage and franchise Holiday Inns, Inter Continental
11 Hotels and Crown Plaza Hotels.

12 All together we have about 3,200 hotels that are
13 distributed across 100 countries, and all of those
14 hotels with just a few exceptions are connected with
15 data networks into our reservation system.

16 That same reservation system is then connected
17 to our web sites. It's connected to travel agency
18 networks. It's connected to a number of mechanisms or
19 call centers, all for the purpose of making it very easy
20 for consumers to inquire about a hotel room, to ask
21 about a price and to book the reservation.

22 We also have a very successful customer loyalty
23 program called Priority Club. We have over 12 million
24 people enrolled in that club, and so we take the privacy

1 and the security of our customers very seriously.

2 A few years ago we made a tremendous investment
3 in the physical safety of our guests in that we required
4 all of our hotels to change their key door locks to
5 the electronic locks, and so we have a history and a
6 culture of being concerned about our guests' safety, and
7 we're very committed to information security.

8 MS. CLAY: Thanks, Lynn.

9 Next we have Frank Reeder. Frank formed the
10 Reeder Group after a career of more than 35 years in
11 public service. Frank is chairman of the nonprofit
12 Center for Internet Security and also chairs the
13 National Computer Systems Security and Privacy Advisory
14 Board of the National Institute of Standards and
15 technology.

16 Frank?

17 MR. REEDER: Let the record show that's a pro
18 bono, and the taxpayers are getting their money's
19 worth. I'm not sure how to take that back.

20 But I would like to parse the problem a little
21 bit differently because we've been distinguishing
22 between businesses and consumers, and as I had listened
23 to some of the previous panels, there's a scaling
24 problem, and certainly the challenges that face

1 Microsoft are slightly different or the capacity to meet
2 the challenges facing Microsoft are slightly different
3 from those facing the small business.

4 And I would really like to focus my remarks on
5 the small business and consumer because I think their
6 problems are probably more similar.

7 The nature of the problems they face in this --
8 at the risk of repeating what you've already heard -- comes
9 from several perspectives, first and foremost from
10 within, from acts of vandalism or acts of inadvertence
11 that run the risk of damaging security, security being
12 defined as the availability, integrity and
13 confidentiality of information, and also secondarily and
14 obviously non trivially protecting themselves against
15 acts of malice from people outside, hackers, a polite
16 term for people who are a combination of thieves,
17 vandals and thugs.

18 The consequences also are fairly obvious. One,
19 financial loss, that is you can lose your money or your
20 merchandise. In the case of a Six Continents, it might
21 be you would lose your ability to sell rooms which is
22 ultimately what they're in the business of doing,
23 interruption of service, a business unable to operate
24 and ultimately loss of confidence by your customers and

1 your ability to continue to deliver reliable service.

2 And here I risk -- I think the automobile
3 metaphor is extraordinarily useful in several respects.
4 We're dealing with a technology like any new technology
5 that has the potential to deliver enormous value and
6 good, we needn't belabor that, but with some unintended consequences
7 and some potential risks that can cause and inflict great pain and
8 loss.

9 To prevent that, we need to do a couple of
10 things. Obviously we need smart people out there who
11 can help us protect ourselves, but as several of the
12 speakers have reminded us, there probably aren't enough
13 smart people out there to populate every organization,
14 certainly not when we start talking about our parents
15 and grandparents' computers or mom and pop store
16 computers.

17 So something else has to happen in this
18 marketplace to assure that those folks don't become the
19 victim of the technology that they're attempting to use
20 for their benefit, so what can you do?

21 One we've already talked about, beat up on
22 Microsoft and get it to build safer products. The
23 reason we beat up on Microsoft is because they're the
24 biggest and by definition, if you were going to hack a

1 product, you might as well hack Microsoft Exchange
2 rather than something obscure.

3 It isn't obvious that their products are
4 inherently weaker, they're just inherently more
5 attractive to people who want to break into them.

6 In any event it's reasonable of us to expect the
7 kind of commitment we're beginning to see from the
8 people who sell us technology to deliver safer products
9 but let's assume that away.

10 Let's assume for a moment that tomorrow we had
11 the equivalent of airbag equipped, antilock brake
12 equipped vehicles riding the information super highway.
13 We would still be left with two other very large
14 problems, one again as was discussed in the panel this
15 morning, the problem of user education.

16 The UL metaphor is wonderful. Even if you buy
17 the hair dryer that has a UL label on it, you need to
18 know not to toss it into the bathtub while you're in
19 it.

20 So it is possible to do harm with safe products
21 and so the notion that delivering a safe product
22 guarantees safety is I think a trifle naive and probably
23 didn't bear belaboring.

24 Initiatives like say Stay Safe Online for

1 example are terribly important. We need to continue to
2 push user education. We need to continue to -- and the
3 safe computing metaphor I think is a very interesting
4 and helpful one, but finally we also need -- and here
5 the automotive metaphor I think is important, a series
6 of things that deal with one, the problem of latent
7 defects.

8 Even the safest product, especially in a field
9 as dynamic as information technology today is likely to
10 be rendered unsafe tomorrow by virtue of the uncovering
11 of defects that we weren't aware of at the time it was
12 delivered or by virtue of the manner in which the user
13 applies that technology, and so you need to do a set of
14 things that even if you were delivering the safest
15 product assures that those products continue to be
16 safe.

17 In the automobile space, we do periodic safety
18 inspections, and we have product recalls when
19 deficiencies are uncovered that are deemed to be of
20 sufficient magnitude to warrant that kind of action. We
21 place a responsibility back on the vendors. We place
22 the responsibility back on the distribution system to
23 correct those defects.

24 And the inspection metaphor I think is also

1 important from another perspective, and that is
2 information technology systems are by their nature
3 inherently complex, and it is imminently possible in the
4 course of doing business to undue the safety measures
5 that may already be installed in the system, and so
6 periodic checking becomes very important.

7 As to what's available out there, there's a
8 range of capabilities that already exist with respect to
9 what we're starting to refer to as minimum standards of
10 good practice. NIST is an important source, and in fact
11 in our conversation prior to this one of the things we
12 agreed upon as a panel was that we would provide, each
13 of us, to the Commission a list of resources that we
14 were aware of that it might -- that the Commission might
15 put on its web site, without endorsing it, as resources
16 that are potentially available.

17 At the risk of being accused of acting in self
18 interest, I would like to mention just one of them just
19 as an illustration of the kind of thing that can be
20 done. About 18 months ago a few of us in a dark room
21 across town conceived the notion of something called the
22 Center for Internet Security.

23 The notion of the Center for Internet Security
24 is very simple. That is that there is a set of -- that

1 most of the vulnerabilities that are being exploited in
2 the Internet are very well known as are the remedies for
3 those vulnerabilities, and that one of the things that
4 we can do to contribute to the level of safety on the
5 Internet is simply sharing through an open mechanism
6 what is perceived to be the consensus on good practice.

7 Not at the level of generality that most of us
8 understand, change your password periodically and back
9 up your files, but at a level of great specificity, that
10 is these are the minimum settings you ought to have in
11 your X operating system or on your Y router.

12 We'll put the URL for the center on this list.
13 This is not a solicitation for support. The center
14 provides its products and its tools free.

15 The final point I would want to make, and here
16 again I come back to the automotive metaphor, and I
17 think it again echoes things that were mentioned
18 earlier. We've got to start thinking about more passive
19 restraints.

20 We have to, as other speakers have already
21 indicated, start to use the technology intelligently so
22 as not to require that every individual or every small
23 business that operates technology systems needs to have
24 expertise. We see folks in a -- I'm not doing this to

1 pander to AOL, I don't make any money from them. AOL
2 has figured out how to push software out to you without
3 your having to do anything. You don't have to be a
4 systems administrator to update your version of AOL
5 because AOL understands to do that.

6 The virus packages that I used Friday told me
7 that Microsoft had three patches out for its browser and
8 showed me where to go to download this with a simple
9 click. It didn't require me to do anything except to
10 respond to a notice that I already got because I'm not
11 prepared yet to allow my virus software to download
12 automatically.

13 Those kinds of things, that kind of technology
14 exists. We've got to make it easier for folks to
15 protect themselves without having to become technical
16 experts.

17 MS. CLAY: Thanks, Frank. Next we have Vince
18 Sollitto. Vince is vice president of corporate
19 communications and external affairs at PayPal. There he
20 oversees public, investor and government relations.

21 MR. SOLLITTO: Good afternoon. I think I must
22 be sitting in the assigned industry seat which is why
23 Simson must have removed my microphone for this
24 segment. Hopefully you can all hear me. Much better.

1 Great.

2 I'm here probably as a quick example of a
3 company that can provide some context about what we have
4 to do for security because of the vulnerabilities that
5 we as a small business online face and also a quick
6 possible solution for some very small businesses that
7 have begun to take advantage of the security we
8 provide.

9 Just before I get any further, I would like to
10 ask a quick question. How many folks have actually
11 bought something online in this room? How many folks
12 are familiar with eBay in here and PayPal, anyone
13 familiar? And how many had the delicious barbecue beef
14 sandwich and will be asleep in about three more
15 minutes?

16 Real quick, PayPal is an online payment service
17 that allows people to send money in a sense by email to
18 anyone else with an Internet connection and an email
19 address. Part of what we do is we allow the consumer to
20 give us their financial information and data and not to
21 the recipient, particularly if it's someone they don't
22 know. That's part of the appeal of the system to a
23 consumer.

24 As such PayPal is a repository of financial

1 information and private information for consumers and
2 for the small businesses that get paid through our
3 system. So PayPal is a relatively new service launched
4 about two and a half years ago. We currently have over
5 16 million members using the system. It's kind of
6 shocking for someone who just joined the company when
7 there was only about 30,000 customers, but about \$3 and
8 a half billion was sent through the network last year.

9 Currently about 300,000 transactions are done
10 every single day. About \$17 million goes through the
11 network each day. People conducting transactions with
12 other people they don't know instantly and securely and
13 part of that reason is our security. So as Willy Sutton
14 said, why did he rob banks, because that's where the
15 money is.

16 That's one of the reasons why we have to be
17 ultra secure because we are where people go to place
18 their information so they don't have to share with
19 others, and in fact we have 16 million accounts with
20 credit card data, bank account information and a whole
21 host of other financial data.

22 Are we at risk? We are certainly a target. As
23 Frank said Microsoft may not be any less secure than
24 anyone else. They're just a very attractive target

1 because they're huge. We're very large, we have a lot of
2 information out there, so we take security very
3 seriously.

4 Fortunately one of our founders is a cryptography
5 expert and actually built the entire system in-house so
6 we don't rely on any outside stuff, and a large part of
7 that is many of our solutions are customized and they
8 work for us.

9 What are some of the important things that we
10 do? Well, all our transactions occur on secure servers
11 using SSL and that's something folks, consumers can look
12 for when they shop on line, is this site I'm on actually
13 a secure site, does it say HTTPS, or just HTTP, and a lot
14 of e-commerce sites don't necessarily take advantage of
15 that, figuring their consumers may not have the ability
16 to access those sites with the best technology or they
17 just don't want to go that route.

18 All the information that comes to our site is
19 entered via SSL, HTTPS, URL, and then what happens to
20 the information after we have it? It sits in our secure
21 servers which are surrounded by firewalls and we use
22 128 bit encryption which is military grade. As a matter
23 of fact our CTO is from Russia so in America it takes
24 two keys to launch a nuclear missile, but in Russia it

1 takes three people or at least three keys to do that or
2 actually it did until they began to become a little more
3 flexible.

4 As a result, whenever we have to restart our
5 database, we have to get three people out of eight
6 together in a room, and they all have to enter in a 128
7 character password which they all have committed to
8 memory so it's obviously a pretty secure system.

9 One other thing we do is we don't connect our
10 servers to the Internet directly. All the information
11 is stored offline in a sense and housed in a number of
12 facilities in California underground, with biometrics by
13 the way, so what does this mean? We still get probed
14 constantly. We get about 500 attacks a day.

15 Now, some of them we pay for. We try and
16 get professionals to try to break in constantly but many
17 others we don't. They're from all over the world
18 Russia, Indonesia and beyond.

19 So security is obviously critical to us. We're
20 very fortunate that we've got some great people doing
21 some great things with it.

22 One of the interesting things about being in our
23 business is we often learn of hacks of other sites
24 before perhaps the victims do themselves because PayPal

1 is a place where people who may have gone and stolen
2 credit card data from other less secure web sites
3 might come in an attempt to use those stolen credit
4 cards and monetize them in a sense, go open up an
5 account with somebody else's credit card, try and send
6 money to someone you know or perhaps even yourself and
7 withdraw it.

8 And in fact we frequently work with the
9 authorities on identifying large bin numbers of credit
10 cards that might have been hacked or compromised, so in
11 a nutshell what that says basically is PayPal is a huge
12 target because we're a huge database. We take
13 inordinate steps to provide security for that
14 information.

15 Small businesses are faced with this same task
16 and yet we're specialists. They're probably not.
17 They're generalists. For a small business the most
18 important thing they focus on is your business, how to
19 convince you to pay them, not how to convince themselves
20 that the security they have for their web site is the
21 best it can possibly be.

22 A lot of people on this panel are going to
23 explain ways and steps business can take to protect
24 their web site and consumers can take to protect their

1 information on their web site.

2 I offer out there as one example of a solution
3 that both consumers and small businesses have come to is
4 that in a sense why not out source that concern to a
5 specialist, and in fact that's what our 16 million
6 members do.

7 Consumers use our system as almost a secure
8 online wallet where they just give only one web site
9 their financial information, credit card, bank account
10 and such, ours, and then transact through us so as to be
11 more secure because they don't have to worry about
12 whether or not Frank's web site, although I'm sure it
13 is, secure so to speak.

14 Same thing with small businesses. They're not
15 really interested in using that information. They don't
16 want it. They don't want the risk or the liability.
17 They just want your money, and so by using our service
18 they don't have to worry about whether or not they've
19 held that information secure.

20 Obviously there are many steps they can do to do
21 so. I'm sure we'll hear more about them. I'm just
22 trying to explain the steps we have to take to secure
23 that data. I know how difficult that is and also to
24 indicate there are other options out there if folks

1 don't feel frankly up to the task.

2 MS. CLAY: Thanks, Vince.

3 Next we have Vic Winkler. Vic is the principal
4 architect for security at Sun Micro Systems public
5 sector. There he's been responsible for enabling
6 customer security architecture decisions, authoring
7 security white papers and writing the security policy
8 for the government of Malaysia.

9 MR. WINKLER: A disreputable place sometimes,
10 Malaysia, that is.

11 I'm not sure what I should say to you except for
12 run for the doors. I think security has collided with
13 marketing, really good marketing in the recent past and
14 for a number of years. It's on the one hand
15 extraordinarily difficult to achieve a comfortable level
16 of security. On the other hand it can be relatively
17 easy to achieve appropriate security.

18 And there were a number of examples today using
19 cars and other objects that can kill bugs, but I think
20 that it is a great challenge to both the consumer and to
21 a small business, even to a medium or a large sized
22 business to impose functioning solutions, manage them
23 day-to-day and have a degree of trust that they'll do
24 what you think they'll do when those solutions are

1 comprised out of components that are unbelievably
2 complex, and that are designed really not to inter
3 operate very well together.

4 In fact sometimes the individual components are
5 designed not to inter operate with other vendor's
6 technologies so at the point where we are today, and by
7 the way, where we are today is a snapshot in time, and
8 we really shouldn't feel too good or too bad about where
9 we are at a particular point in time, right?

10 So if we look back at an archeological record
11 we'll find mainframes which were the scenes of much
12 control and tyranny if you had an application you wanted
13 to run on them, and then enterprises managed to wrestle
14 away certain modest amount of funds from their financial
15 officers and bought mini computers where they could then
16 run applications without the constant attention to
17 detail that one had in the main frame world, and then
18 all hell broke loose.

19 PCs appeared. This was the cause of much chaos
20 and much confusion trying to move from one PC to another
21 to just do your damn work, right? Then after that the
22 network slowly caught up with PCs, and we found we could
23 move things around, and since then it's been a blur.

24 I'm not sure where we are today, except that

1 things seem to be moving up into the network and away
2 from all of these little computers that we have sitting
3 at our desks. These are just -- they seem to be, and
4 these little devices that can communicate with the
5 network seem to be just little port holes into the
6 network for information and applications.

7 That kind of a world seems to me to be far
8 easier to manage from the standpoint of controlling
9 enterprises and what individuals can do than does the
10 world where applications and data all reside on
11 individual platforms. Where all the data and all the
12 applications really have to reside on individual
13 producer platforms, that's untenable. That can't be
14 managed.

15 The amount of code that can't be proven for
16 correctness and authenticity, that you can't perform
17 that on each of those platforms. We're not at that
18 point. Theoretically it's very far off, so the model
19 where we have centralized control over applications and
20 data but where users can have exactly the same rich
21 computing experience that they have today but without
22 all the hassles, and you might not want to ask yourself
23 where you want to go today but rather what you want to
24 do today.

1 And if what you want to do today involves fixing
2 bugs, patching, fighting viruses, fighting hostile
3 things over the Internet, I don't want to play that
4 game. I want to play the game where the computer
5 resources I use are tools that allow me to do my work,
6 and that's the same for a consumer as it is for a
7 business.

8 It's sheer lunacy to expand the tens of millions
9 of dollars that the Veterans Administration said they
10 spent last year fighting two viruses. That's a
11 phenomenal amount of human effort, amount of resources
12 in the economy that are being poured in one direction. It's a
13 tremendous waste of human effort, and computers really have the
14 potential just like television once upon a time did of enriching our
15 lives.

16 And we're at the same point today I think where
17 television was a number of years ago when Madison Avenue
18 got a hold of it. It became something that was marketed
19 to the point where your television viewing experience
20 without Tivo is a terrible thing, and that's the
21 convergence of computing and TV.

22 Now I want to see the convergence of reasonable
23 behavior and reasonable architectural choices with
24 computing, and I think that's all I want to say right

1 now.

2 MS. CLAY: Thank you, Vic.

3 Last but not least on the panel we have Marc
4 Zwillinger. Marc is a partner in the Washington office
5 of Kirkland & Ellis, a cyber law and information
6 security practice group, and he's a member of the firm's
7 technology committee.

8 MR. ZWILLINGER: Thank you. The panel is book
9 ended by lawyers. I guess I have to start with the
10 reverse disclaimer, which is that I am a lawyer, and I
11 know nothing about anthropology.

12 As a lawyer, what I do is I help my clients
13 handle computer incidents, that is I help them prevent
14 and minimize and recover losses for when a computer
15 incident occurs, and I deal with relatively
16 sophisticated clients.

17 And where I find that they have the most
18 problems in preventing computer losses or recovery
19 losses is in incident response, that is in handling an
20 incident after it's occurred and recognizing it and
21 responding to it.

22 And the panel that we're talking about is
23 entitled "what steps can businesses that maintain
24 consumer information take to improve their own

1 security?" So talking about incident responses doesn't
2 seem to make that much sense because already there's
3 been a problem, but we know there's going to be a
4 problem because no preventative measures are 100 percent
5 effective, and if we look at the Security Institute and
6 FBI study this past May, last year 80 to 90 percent of
7 the companies that responded reported some kind of
8 security breach.

9 So my perspective on that is that a proper
10 response can help reduce losses both for the business
11 and for the consumer, that is for the business, the
12 response to an incident may be more significant than the
13 incident itself.

14 That is you take the CD Universe case for an
15 example. Credit card data was lost and had the company
16 wanted to make good on all the credit card transactions
17 that occurred as a result of the stolen data, they could
18 have done that without even affecting available cash,
19 but because the incident was so well publicized, because
20 they didn't handle it as well as they could have,
21 because the marketplace stigma that got attached to it
22 led to the demise of the company, the handling of the
23 incident resulted in the demise, not the actual
24 penetration.

1 From a consumer point of view it's the same
2 thing, that is if a company recognizes signs of attack
3 right away and responds appropriately, what could have
4 been a simple penetration or trespass defense can be
5 stopped there. If there's no proper response it can
6 result in full theft of credit card data, trade secret
7 loss for the company, consumers with out of pocket
8 losses and a near catastrophe.

9 So since the ticket to this debate seems to be
10 being able to make automotive analogies, I have to say
11 what I'm talking about is like Lojack, that is your car
12 is taken, and you limit your losses and you get your car
13 back by being able to handle the incident, call the
14 police, track the car and get it back to you, assuming
15 some percentage of automobiles losses are going to
16 happen, your car is going to get stolen no matter what
17 security you put in place.

18 When we talk about incident reports, I want to
19 focus on the two aspects of it, which is recognition and
20 reaction, and I think it was Laura Berger in moderating
21 the last panel that asked the panelists to talk about
22 the problems of recognition from a consumer point of
23 view, and there are problems in recognition from a
24 business point of view as well. That is, it's difficult

1 to separate the incident from the background noise.

2 You have to have a lot of experience with a
3 system like PayPal to know that it's normal to get 500
4 attacks a day and what those attacks look like and what
5 bandwidth they consume, so when you're seeing one day
6 1,500 attacks that all seem to be coming back to a
7 country where you're not used to seeing that amount of
8 traffic, that something is going on and to react
9 appropriately right then.

10 The problem is we have a difficult culture even
11 in businesses with users recognizing these problems,
12 that is we've lived in a situation, and I'll bash
13 Microsoft for a moment, where we blame our problems on a
14 computer system with Microsoft's operating system so we
15 say, Well the computer crashed but that's Microsoft. It
16 doesn't occur to you, your first instinct, that the
17 reason your computer crashed is you just suffered a
18 denial of service attack. You just try to reboot and
19 only after a couple days of a problem that the staff
20 can't fix, then you start to think about other causes.

21 The network is slow today. Sometimes that
22 happens. The network is slow. Also the network can be
23 slow because your bandwidth is being consumed by people
24 that are taking over your computer systems and are using

1 it to launch denial of service attacks.

2 So getting businesses to train their own
3 employees when an attack is taking place is often
4 difficult and requires planning and thought.

5 The most famous example is Cliff Stohle for the
6 people that read the Cuckoo's Egg. He noticed this
7 infiltration into the computer systems there by noticing
8 a 75 cent discrepancy in the accounting system, realized
9 somebody had created an account. On one computer that wasn't on
10 another which resulted in a 75 cent discrepancy, and when he found out
11 why that account had been created it was a hacker who had broken in and
12 got administrative privileges, and the
13 whole investigation started from that simple discrepancy.

14 That's what we need in our corporate
15 environment. That's what we need for businesses to
16 protect themselves and to protect the consumers.

17 And again the analogy doesn't always work and
18 here it breaks down because when your car is stolen, you
19 tend to know it. You walk out of the mall and you utter
20 those words that have been made into a movie this year,
21 Dude, where's my car, right, but you don't do that in a
22 computer environment.

23 You don't know that your system has been
24 penetrated and you don't what's been taken which is why

1 the next phase I want to talk about briefly, reaction,
2 is so important.

3 That is without a plan in place, a plan that
4 requires the assembling of a multi disciplinary response
5 team, you're never going to be able to respond to an
6 incident quickly. You don't want to be making
7 introductions, and I'm not going to beat up on PayPal,
8 but I'll use them as an example.

9 Vince doesn't want to meet all the people both
10 inside and outside who are going to be needed to respond
11 to an incident after the incident occurs. He wants to
12 have worked with them and planned with them and set out
13 a strategy and protocol well before he experiences a
14 system penetration.

15 You hire a law firm to respond, you can't even
16 clear conflicts in the first 24 hours much less get a
17 retainer on file, right? So you want to be putting your
18 teams together in advance.

19 The other aspect of the team is involving
20 outsiders. Nobody wants to spend a lot of money
21 responding to incidents, and your plan or protocol will
22 tell you when you need to kick it into high gear.

23 If we go back to the Computer Security Institute
24 and FBI study last year 150 million dollars of losses

1 were caused to 200 companies from insider theft or
2 insider abuse. So when you detect your incident, is
3 your first call going to be to the insiders who are
4 going to investigate and tell you what happened, or are
5 they going to be to an outside consultant who's going to
6 come in and do an analysis.

7 These are all questions you want to think
8 about. What types of incidents do you want to respond
9 to in one way, what types do you want to respond to in
10 another way because only by getting that done before an
11 incident occurs will you be able to respond effectively
12 and cut your losses.

13 The only other thing I want to mention at the
14 beginning is the problem of attribution. That is,
15 companies tend to respond to a computer incident of any
16 type with a make it stop approach, that is I don't know
17 where it's coming from but let's just make it stop, and
18 making it stop often amounts to closing your eyes. That
19 is you want to know before you make a decision on
20 responding to an incident whether this is a competitor
21 or a malicious hacker, whether this is a teenager, and
22 even the government has trouble with attribution.

23 I've been involved in a couple of cases, excuse
24 me -- I'm trying to give the stenographer a run for her

1 money. I've been involved with a couple cases in the
2 government where in the first 24 hours after an attack,
3 there was a conclusion reached, tentative conclusion
4 reached that this was an organized attack, this was a
5 nation state trying to break in to the computer systems,
6 when several days later this same attack was properly
7 attributed to teenagers in California.

8 I've been on the other side as well, that is an
9 entity didn't respond quickly and said it's just kids
10 when it was in fact organized criminal activity, and if
11 you don't think about how you're going to solve your
12 attribution problem, you're going to end up in a
13 situation where you have losses and you have to explain
14 those losses to somebody, to your customers, to your
15 vendors, to Congress, as to why you didn't respond
16 quickly because you thought it was just kids and it
17 wasn't that important.

18 You need an attribution strategy as part of your
19 incident response plan, and all of that together gives
20 you a way, whether you're a small business or a large
21 business, to minimize your losses. If it's two people
22 in the company, your plan could be when do you call the
23 other person, when do you call your outside provider,
24 your ISP to say, Help us, but you need to have thought

1 about that in advance as a way to minimize losses.

2 MS. CLAY: Thank you, Marc.

3 Marty, you look like you're itching to say
4 something before we go on with the questioning.

5 MR. ABRAMS: I am. I've spent many years trying
6 to arbitrate disputes between marketing departments and
7 security departments in organizations, and one of the
8 things I mentioned before that security can't get in the
9 way of immediacy, and in the world in which we live,
10 often there is a disconnect between the concepts of
11 security as we have we mapped them out and the concepts
12 of reacting to a marketplace where people buy because of
13 quality, price, quickness, all of those attributes.

14 And part of that conversation, part of this
15 whole question of reinventing the way we think about
16 talking about security and where we place security I
17 think was mentioned by the gentleman from Sun Micro
18 Systems, that we need to find ways so that it's not
19 about stopping the process. It's not about slowing down
20 commerce.

21 It's about building the infrastructure that
22 allows us to have security work without people having to
23 work AT security.

24 MR. WINKLER: Yes, and I would like to follow up

1 and say that our architectures, the Internet, large
2 businesses, these architectures have grown organically
3 without very much planning in advance. They've been
4 kind of added on to and so forth, and what we need to do
5 is step back and rethink what these architectures are
6 really supposed to do for us, not how we can best serve
7 them by buying more products that fit in here and there
8 to try to better protect things that are inherently
9 defective or ways of doing things that are inherently
10 defective or counterproductive.

11 MS. CLAY: Your introductory statements have
12 been a great lead in to this afternoon's discussion.
13 One of our goals is to close out this session with a
14 clear understanding of the real issues that businesses
15 are facing and some ideas or even examples of how they
16 can address those issues, and a lot of that or at least
17 some of that has come out already.

18 So with the first question, let's say that we've
19 been asked to start a list of processes that businesses
20 should implement to secure consumer information. As a
21 base line, what would you put on that list? What would
22 you include?

23 MS. GOODENDORF: I'll start out that one of
24 the processes that is so critical for businesses, very

1 basic, is a risk assessment, and every business, every
2 industry is going to be a little bit different, and when
3 you do a good job on risk assessment, then you really
4 know where to focus your security energy and where you
5 should spend your money and what you should spend it
6 on.

7 That's just one process but I will start with
8 that.

9 MR. REEDER: In the interest of provoking a
10 little bit of controversy, let me disagree, and it's a
11 partial disagreement because certainly risk assessment
12 is not -- is an important tool of security management,
13 but I would start in a very different place, and that is
14 there is a set of base line practices that irrespective
15 of the risk that one is assuming, obviously if you're a
16 bank you're in a slightly different place than if you're
17 a public library, but everybody needs to worry about
18 availability.

19 And so there is a set of things that every
20 organization needs to do. I'll diverge from cars to
21 medicine. We all know that we ought to wash our hands,
22 that medical practitioners probably ought to wash their
23 hands between patients. It doesn't guarantee that
24 infection won't be transmitted, but there's a level of

1 risk that none of us need to assume even assuming that
2 nobody that we're dealing with that day happens to be
3 infected because we simply don't know.

4 So I would start in a slightly different place,
5 and we could all construct our own list. We all need to
6 do things like back up. We all need to do things like
7 making sure that our software is up to date. I would
8 argue that you ought to look for the Center of Internet
9 Security benchmarks which are designed as minimums.

10 What I fear and I don't think -- and I'm putting
11 words in to Lynn's mouth that I don't think are
12 necessarily hers. What I fear is if we walk out saying
13 you ought to do a risk assessment, everybody feels
14 comfortable, now, I can wait six moments until the
15 consultant's report comes back and I have an idea what
16 my risk is.

17 There's a shared risk that we all have by virtue
18 of living on the Internet and a set of things we ought
19 to be doing while we get the consultant in that says to
20 us -- and beyond that because you are who you are and
21 because your business is so heavily dependent on
22 availability, there is a set of things you need to do.

23 MS. GOODENDORF: I don't disagree, but I would
24 say that a lot of companies have comforted themselves by

1 spending a lot of money on security, but if they spent
2 it -- particularly buying a lot of tools and doing this
3 and that, and they're thinking that they're doing a
4 great job, and some companies will benchmark themselves
5 on how much money they're spending on security, but
6 they're not necessarily spending it on the right things.

7 And I think that's the whole point of really
8 just thinking through where your risks are and where
9 your vulnerabilities are.

10 MR. WINKLER: I think the problem with risk
11 assessments is that it doesn't much matter whose
12 assessment you read. It probably will apply to your
13 environment, and that the risk assessment industry is --
14 while there are some very capable practitioners, it's
15 going to make a lot of money doing very little except
16 changing words with some boilerplate.

17 So I think the point about best practices is
18 probably the one I would lean more towards, if I can
19 change what you said and call it best practices, a base
20 line of accepted ways of doing things. And I think that
21 we would all do better with more attention to that.

22 MR. ABRAMS: Again part of where I'm getting
23 uncomfortable in the discussion is we're separating what
24 we're trying to do as an organization from the whole

1 question of how we're safe as an organization, and in
2 the area of helping organizations think through their
3 information policy, we say you should catalog your risks
4 along -- in four bundles, okay?

5 And the first bundle is compliance risk, and
6 let's put that aside. The second is reputational
7 risks. What are the things that if they go wrong will
8 put you in a position of losing your brand, your ability
9 to work with the outside world?

10 The third is investment risk, and that goes to
11 the whole question of if you have a problem, how will
12 that affect the payoff on your business going forward,
13 and the last is reticence risk. What are the things
14 that if you're reluctant to make decisions will make it
15 difficult for you to do business with the folks that you
16 need to do business of going forward?

17 In my interaction with the whole question of
18 security, typically we never get to this question
19 of reticence risk, and what happens in organizations
20 that if the security tool is too hard to use or gets in
21 the way of that interface with the consumer, if the
22 consumer has to wait too long when they come to the
23 Inter Continental site to do whatever it is they want to
24 do, then what happens is that the security stuff gets

1 turned off, and then you actually end up with more risk,
2 which is sort of why we need to think about the whole
3 question of security as integrated into the business
4 process and not something that is left to, quote, the
5 specialists in information security.

6 MS. GOODENDORF: I think someone on the previous
7 panel made a comment I strongly agreed with. He said
8 the best security -- I don't remember his exact words
9 but it really enables the business. It doesn't hinder
10 it. It enables it, but I would just mention other base
11 line processes that I think should be mentioned is
12 prevention, which includes patch management.

13 And I was talking with someone a few weeks ago
14 about the importance of patch updates which is a
15 preventative measure and he said, Oh, that sounds
16 kind of going like to the dentist. It's not glamorous.
17 It's not jazzy. People in the technology industry
18 aren't particularly attracted to that.

19 It's like maintenance, and yet most of the
20 vulnerabilities, a lot of the security breaches that are
21 happening are exploiting just known vulnerabilities that
22 can be prevented with patch updates.

23 Detection I think is another base line process
24 that is significant, and intrusion detection has come a

1 long way in its capabilities, particularly in the past
2 year, and there's both network intrusion detection and
3 host intrusion detection, both of which address -- I
4 can't remember who mentioned it, but companies not even
5 realizing that something has happened.

6 Those are probably the most insidious security
7 breaches are the ones that you don't even know that are
8 going on, and I think that's really the value of
9 detection of recognizing when something's abnormal and
10 attacking it and then also I agree about response plans
11 too, I consider that another category of base line
12 processes.

13 MR. ZWILLINGER: If I might, and my comments are
14 always going to be in this vein of sort of thinking
15 about security from both the technological and the
16 policy or legal point of view. I think it's very
17 important to recognize that when you deploy technology
18 of any sort, you need to do it with policies, that is,
19 three basic policies are external facing policies, your
20 terms of service, your internal facing policy, what's an
21 acceptable use of this technology on your networks, and
22 your incident response policy, what are the base line policy
23 processes and do they support your technology.

24 That is again to my point, you can put into

1 place whatever system you want. An insider can exploit
2 it, but if you have an ability to monitor that insider's
3 traffic, when they start to exploit it, you can detect
4 it and stop it even though your IDS system doesn't
5 necessarily go off or stop it itself so those are the
6 three base line policies I would introduce into the
7 process.

8 MS. CLAY: Would anyone like to make a comment
9 on training before we move on to the next question,
10 training with respect to a process that should be
11 implemented for business security? Anyone? Anyone.
12 I'll make a comment. This is one of the fun things
13 about having the mike.

14 I think that this is one of the things that was
15 mentioned earlier today is that we can have a lot of
16 technology out there, a lot of processes in place, but
17 if the people who are responsible for getting the job,
18 the ultimate job which is making new sales, if they
19 don't understand what they're using and why they're
20 using it, then you can still have a huge security
21 problem because there's always a way to work around that
22 little thing that the security officer wants you to do,
23 so just another thing to keep in mind.

24 The other thing I would like to mention is that

1 some of the topics that have come up just in this first
2 question about risk analysis, risk management,
3 contingency planning, security policies, you will have
4 access to resources on how to start with some of those
5 things.

6 That's one of the things that we'll provide to
7 Mark to put on the FTC web site.

8 MR. REEDER: Alicia, if I may, I think it's
9 important to distinguish between organizations of
10 sufficient size that they can, for lack of a better
11 term, attempt to create a security aware environment
12 where security awareness training is built into the
13 normal mechanisms.

14 But ultimately I'm not saying about our ability
15 to take the small business person or our proverbial
16 aging aunt or uncle who's gotten that \$600 PC and is now
17 email enabled and talk a lot about training.

18 I think we really have to think more about what
19 I would call passive security, that is, doing things
20 that -- and here the metaphor actually works. We build
21 cars that are safe. We teach people, we try to teach
22 people how to drive them safely, and we still expect
23 them to run into other objects and so we do things so
24 that when that occurs they don't hurt themselves as

1 badly as they otherwise might.

2 And we increasingly try to do that with side and
3 front airbags or rather than even having them --
4 although we know we should use seat belts as well,
5 relying on their willingness to always do that, and I
6 think we have to think that while training is terribly
7 important and certainly in enterprises of any size it's
8 feasible, I think there's a limit of how much awareness
9 and training can accomplish, and given the power we're
10 putting in to the hands of folks who aren't going to
11 worry about that.

12 MS. CLAY: Very good point, Frank, and I think
13 that the closer we get to that point about passive
14 protection, the better off and the more enabled we'll
15 be. Very good point.

16 Are there any standard software or hardware
17 elements that should be included in a good security
18 program? If so, what are they?

19 MR. SOLLITTO: Well, at the risk of redirecting
20 the question or sort of almost rebutting in a sense, I
21 think one thing you folks should keep in mind is that,
22 maybe this is the same conflict about whether you do a
23 risk assessment or whether in fact there are basic
24 standards that all folks should do, that at least in our

1 experience we found that what we do for security is
2 what's right for us.

3 And I'm not sure that there is a general basic
4 standard that is the best for each company, each
5 customer, or just general use because as was talked
6 about before down here, if somebody goes to this hotel
7 site and can't log in because we've made it so secure
8 that it's virtually unusable, then that company is going
9 to be out of business.

10 And part of the reason our company has been so
11 successful in our view is because we've struck a balance
12 between convenience and security that works for us and
13 our customers. For us it's a really high hurdle because
14 we have to be really secure and still very convenient,
15 and I think it's just important that folks realize that
16 security is inseparable from the way a business operates
17 and the business goals at hand, and that what works for
18 some folks might not work for others, and that we've
19 basically been forced to advise what works for us of
20 separating unique situations.

21 For instance, I'll take one example. All the
22 transactions that occur on our web site occur via SSL
23 technology, secure socket. EBay does not do that. They
24 have decided that the transactions that occur on their

1 site require less security than perhaps we might because
2 of the financial nature of ours versus the pure
3 commercial nature of theirs, that combined with the
4 broader user base they may have or the inability of all
5 of their customers' technology systems to interact
6 ideally in that environment and therefore have chosen to
7 go another way.

8 So I think while I would recommend SSL for all
9 types of security, there are very many companies out
10 there who decide that it's not going to be the best
11 thing for them, so I'm sure there's some great answers
12 here on this panel of what might would be the basic
13 standards of security most companies would strive for.

14 I would throw out as a caveat in the beginning
15 that many companies might find that what's best for them
16 is best for their unique situation. I know we certainly
17 have.

18 MS. CLAY: Vic Winkler?

19 MR. WINKLER: There are a number of things that
20 I just heard mentioned that I might have comments on.
21 The SSL issue is one where SSL was originally designed
22 more to create -- allow for the creation of an encrypted
23 link between a client and a server, but the real
24 emphasis was on allowing the consumer at the client end

1 to trust the server, and this is a little bit different
2 in an example like eBay where the trust issue is one of
3 individuals doing business via third party eBay, and I'm
4 not a big fan of eBay but I think there's a difference
5 there.

6 I think the best in terms of standards today
7 really is the common criteria which NIST I think
8 has ownership over within the U.S. in conjunction with
9 NIAT. The common criteria are a set of standards for
10 looking at both the assurance and functionality of
11 security within products, be they operating systems,
12 firewalls, whatever.

13 And it is really up to the business community,
14 the health care community, the consumer community to
15 define what are called protection profiles, which
16 operate against them.

17 So what really hasn't happened is that we
18 haven't taken advantage of what the common criteria
19 offers in terms of allowing us to define and then value
20 pick products that are in compliance with what would be
21 commonly accepted behaviors or functionalities for a
22 particular domain such as a retail outlet with a web
23 facing the front end.

24 So I think the common criteria really ought to

1 be given more emphasis. There is a lot that has been
2 done in security, and we've really raked most of the
3 hard questions over a lot of coals for many years and
4 have seen that they have not been adopted for usually
5 the wrong reasons, not because security is too
6 encumbering.

7 MR. ABRAMS: In some ways we're talking about
8 the apples of security and the oranges of security.
9 There's certain issues --

10 MR. WINKLER: Can we refer to the apples and the
11 suns of security and so forth?

12 MR. ABRAMS: How about the kumquats and the
13 apricots? That gets us out of brands.

14 In terms of the apricots of security, that's
15 some of the issues that have arisen because of the
16 network world, and I have a great deal of confidence
17 that we can come up with the solutions to those, and
18 build in things like the firewalls that we talked about
19 earlier today.

20 I'm not at all concerned that our ability to
21 come up with technological answers that respond to
22 those issues and our ability to come up with standards
23 will indeed come to the forefront, that there's a will
24 to solve the problem and then it will be solved.

1 I'm more concerned with some of the standard
2 business facing -- consumer business facing security
3 issues that are a lot harder to do with technology. The
4 simple concept of if I don't know you today and I didn't
5 know you yesterday, how do I know that you are who you
6 say you are, and the whole question of how we do
7 authentication authorization in our marketplace where we
8 have lots of other countervailing issues, issues of
9 privacy, issues of people's memories, issues of we don't
10 have -- if we're not going to accept a chip embedded
11 behind our ears, which I think none of us are willing to
12 do, how are we going to build those solutions because
13 it's not just technology based?

14 I think those are the more difficult solutions
15 and the more difficult questions for that small business
16 that truly is trying to safeguard the consumer, the real
17 consumer, not the fake consumer, and the business from a
18 continuous string of fraudulent transactions.

19 So I think in terms of talking about the
20 business solutions we need, I think we have to separate
21 the kumquats from the apricots and let's say, Yeah, we
22 have one approach to the kumquats which is securing the
23 network and securing the interaction with the network.

24 But I still think we have a huge challenge in

1 terms of the second set of issues, which are that we are
2 really moving to an economy where the consumer spends
3 more time serving themselves by interacting with the
4 company directly and not interacting with an individual
5 that says, Hmm, this patient just seems suspicious, and
6 I think before moving forward we separate those two
7 sides.

8 MS. GOODENDORF: I think there have been some
9 common themes in the discussions today that I don't know
10 if they're recognized as hardware and software
11 standards, but it seems generally recognized that
12 passwords have become a standard. Anti-virus has become
13 somewhat of a standard and I think firewalls, and
14 almost everything I see both in the consumer world and
15 the business world, those are three very common themes.

16 MS. CLAY: Okay.

17 MR. ABRAMS: That's a great example. Let's look
18 at passwords, and I'm 52 years old. I fully admit to
19 being 52 years old. Probably the most used button when
20 I go to a web site after I haven't been there for three
21 weeks is have you forgotten your password, and then they
22 ask me such a great question as, What was the first car
23 that you owned.

24 Well, was that the first car that I really want

1 to forget when I was in college or the first car that
2 parents gave me when I graduated from college or the
3 first car I actually paid for? It's a question that for
4 the life of me even if I think about it honestly and
5 rack my brain I just can't answer.

6 Those are the types of things that we -- that
7 we're getting to because things like passwords just
8 aren't working very well today as people like myself get
9 older and can't remember the 16,000 passwords that we're
10 confronted with.

11 MS. CLAY: Marty, it feels like you want to make
12 another statement around what might be an alternative
13 maybe, software, hardware elements for a security
14 program for authentication specifically?

15 MR. ABRAMS: Well, I think there were some
16 suggestions today. I don't have a great answer, and I'm
17 not a technologist, but I think that we have to move
18 towards tools that we can possess, that we can use, that
19 we need to build the utility into our machines.

20 I think the suggestion this morning from Dick
21 Clarke at the Department of Defense, they've solved the
22 problem of people not being able to remember their
23 password by using a token. I think that we need to be
24 thinking about those sorts of tools for the interaction

1 between consumers and smaller businesses.

2 MR. WINKLER: Actually with the Common Access
3 Card, the user still needs to know the pin to unlock the
4 card on which is embedded a very long private key and
5 other information.

6 MR. ABRAMS: But does it liberate the idea of
7 remembering 16 pins or 17 or however many.

8 MR. WINKLER: Yes. In fact, and that depends
9 entirely on -- this is a technological sidelight. There
10 are different smart card formats, and certain ones allow
11 you to lay down different kinds of information and
12 change it under control by the user, and this control
13 issue is one that really touches as both the consumer as
14 well as the business because businesses are --
15 businesses and their relationship of the Internet have
16 changed dramatically and are continuing to change with
17 the concepts of network identity now and how that can be
18 exploited by businesses to allow for a richer, perhaps
19 even better consumer experience as they relate with
20 their digital world different affinity partners,
21 airline, bank, et cetera, and being presented with one
22 perspective without having to sign on to multiple
23 accounts, this will add additional responsibilities,
24 raise the bar for the security at each of the partners

1 that engage in this affinity program where this
2 information is not necessarily shared but aggregated as
3 it's presented to the user.

4 So it's becoming even more complex which I think
5 begs the question, how does one simplify the overall
6 difficulties that are inherent in architectures and
7 computing platforms, and it really comes down to where
8 information and applications need to live.

9 And that's the fundamental question that's the
10 same for consumers at home as well as small businesses,
11 large businesses as well as partners, so the question
12 is: Where does what live and how does it get updated
13 are very, very essential questions?

14 MR. REEDER: I would add here, I'm not also in
15 Vince's employ, but Vince made an important point, and
16 that is especially for the small business and for the
17 individual, you have to make a judgment as to how much
18 of this you can afford to do for yourself and how much
19 of it you're going to simply have to rely on others to
20 provide to you, whether it's going to PayPal for
21 payments because you're not prepared to develop the
22 infrastructure to provide that protection for yourself,
23 or looking to your ISP.

24 And here again my friends at AOL, they can be my

1 poster child, but there are others because putting
2 yourself in their hands gives you a certain level of
3 assurance that you don't have if you're simply going to
4 go it alone on the Internet.

5 There are obvious trade-offs. There are obvious
6 costs in doing that, but part of what we need to do -- and
7 here we need the education of a different sort. I mean,
8 again metaphors sometimes distort. A few of us, myself
9 not included, occasionally lift the head of -- lift the
10 hood of our cars and look to see what's in there.

11 I've actually owned a car for two years and to
12 the best of my knowledge I don't think -- I couldn't
13 tell you where the hood latch is. It's not that I'm not
14 interested in this as a matter of theory, but I know I'm
15 completely incompetent to deal with it, and I'm prepared
16 to pay a certain price to somebody who periodically
17 maintains it for me including doing all the appropriate
18 safety checks.

19 But I understand that that needs to be done and
20 that I have to make an explicit choice as to whether I
21 assume that responsibility for myself or pay somebody
22 and in this case proactively actually take my vehicle,
23 while it turns out with this vehicle it tells me when I
24 need to go visit its other home.

1 That is part of what we're talking about, so
2 again we need to be very careful when we talk even about
3 defining what are the minimum set of things you need to
4 do to be a little more precise about the home we're
5 talking about, whether we're talking about Sun or
6 Microsoft or eBay or PenPal -- PayPal rather as users of
7 technology, not just deliverers of services but as users
8 of technology or again the small sole proprietorship or
9 partnership or our aging aunt on using email.

10 MR. WINKLER: I think that those are very, very
11 good comments, and a business has to ask itself what its
12 core competency is and what it should grow to be, and if
13 its core competency evolves into fixing bugs, updating
14 software and so forth, it's ridiculous. You're always
15 spending your time doing the wrong thing, so that would
16 become the point where you either go to out source or
17 have professional services manage your computer
18 infrastructure or go to a different scheme, and there
19 are different schemes.

20 MS. CLAY: Speaking of, one of the things that
21 you mentioned just a few seconds ago, was keeping
22 systems up to date, and we've also throughout the day
23 we've talked a lot about patching. How are businesses
24 actually accomplishing that now? Do you think that it's

1 being done regularly, daily?

2 MR. WINKLER: As a vendor we have seen many of
3 our customers with exactly the same problems. They will
4 come to a point where they have looked at patches, and
5 there are different approaches towards patching. You
6 can either -- a vendor can choose to release a patch
7 that's unproven almost immediately, or a vendor can be
8 somewhat more circumspect and release a work around
9 immediately and release a patch that that vendor
10 believes will not break other things running on that
11 system, and so that's the vendor aspect of it.

12 Then there's the business aspect where you need
13 to know if you -- you need to decide if you're going to
14 trust a particular patch and whether it will run in fact
15 with your legacy software that you inherited from your
16 great grandmother back in 1802, right?

17 There are a lot of customers who have software
18 that's antique and so you need to decide, and then the
19 question is how do you -- and this is where our
20 customers have a major problem. How do you know that
21 your systems after you patch them are still patched
22 because customers will reinstall software and then miss
23 the appropriate patches?

24 So the U.S. Army, for instance, a number of

1 years ago discovered that even though they had very
2 strong requirements for maintaining a patch program for
3 each and every one of their systems, they found that
4 systems kept getting reinstalled, and the patches failed
5 to be applied to them.

6 So this is something that is extremely
7 challenging for a vendor from a public relations
8 standpoint because you have vulnerabilities in user land
9 that you may have put patches out for years ago that are
10 no longer being carried forward so it's extremely
11 difficult.

12 There is a strategy, and that is to only install
13 software from computers on your network that you
14 control, not to control -- not to install software from
15 external networks or from vendors' networks without
16 putting it on your systems first, making appropriate
17 images and then loading those images on to appropriate
18 platforms in your enterprise.

19 This is something that's extremely cost
20 effective for a business or a large enterprise to do
21 because it allows you to do it once, define what that
22 image ought to be for a specific machine or set of
23 clients, and then if anything requires downloading
24 again, you simply go to this well known place. You know

1 what to download. It happens, it's proven. You don't
2 have to go and change and make sure you don't make
3 mistakes when you select different things, and it's
4 proven to be effective and a number of vendors do this
5 sort of thing.

6 MR. ZWILLINGER: Combining the last two
7 responses, the question was what do people do now for
8 patches, and before that we were talking about out
9 sourcing. A lot of my clients rely on managed security
10 services that do continually scanning of their networks,
11 and they notify them every time a computer goes up or
12 down.

13 The scanning runs pretty much continuously, and
14 they have access to log into a web site to get an
15 instant glance what the network looks like right now,
16 what systems are online, and they can drill down to any
17 system, figure out what version and what software is
18 running by virtue of the managed security services
19 running and really keep tabs on their network.

20 And while that requires some sort of investment,
21 it's not an expensive way to go about it. It's not
22 something for a small mom and pop operation. At the
23 same time it really shifts all the burden and all of the
24 technological know how to an inventor, and at the same

1 time putting out that information right at your
2 fingertips so you can look in at a secure portal, and
3 that's how my clients rely on and make sure their
4 patches are just changed, in charge of reviewing those
5 reports to see what version, which system patch -- it
6 doesn't do every piece of software but it does the ones
7 they're most concerned about.

8 MS. CLAY: I think Lynn and Frank.

9 MS. GOODENDORF: I would say that I'm in user
10 land, that what has worked well for us is rather than
11 the information security grid being responsible for
12 patches, we actually have the various operational teams
13 who look after and operate these systems responsible for
14 that. We hold them accountable.

15 We do have third parties run vulnerability
16 testing as well, but as far as who actually is tasked
17 with doing those patches, it has worked well for us to
18 have that reside in operational teams because they are
19 the most thoroughly familiar with the system. They want
20 it to be up and performing well. It fits well with
21 their other duties so that has worked for us.

22 MR. REEDER: Again, looking back on things that
23 both Vic and Marc said, the Center for Internet Security
24 that I described earlier puts out security benchmarks, one

1 aspect of course is patch management, and most
2 important puts out software tools that are non
3 intrusive, that measure where the systems are against
4 these benchmarks. These again are available without
5 cost on the web site, so that the user can continuously
6 measure not only whether the system settings are as they
7 were originally set but whether they continue to be.

8 But I say that with the important caveat that
9 that doesn't help the individual consumer or the small
10 enterprise for whom that would be beyond their technical
11 skills. It certainly works.

12 MR. ZWILLINGER: Although it does help the
13 individual consumer, again in the context of letting
14 them know who they're doing business with, to the extent
15 you're a consumer and you're getting your financial
16 information to a site, the sites that are running
17 management security services or using the software
18 you've talked about, sometimes you can see that in the
19 organization.

20 They have announced that. They have a seal.
21 They have some sort of way to tell consumers this is
22 what we're running.

23 MR. REEDER: And my not so secret agenda for
24 what I hope comes out of the series of conversations

1 that the Commission has begun is if you will have better
2 information in the marketplace for consumers about the
3 level of security that they're buying when they engage
4 in a relationship with a supplier.

5 It seems to me ultimately the difficulty is not
6 that smart people don't already know what to do, but
7 that an awful lot of people use technology that they
8 shouldn't have to worry about it, who shouldn't have to
9 think exclusively about it, but then don't understand as
10 they do with automobiles or airplanes or selecting a
11 medical care provider whether this individual is
12 licensed, whether they really had been inspected
13 regularly by some accrediting body where the other cues
14 that we understand to look for when we purchase other
15 services that are both critical to our existence and
16 have the potential to harm us if they're not provided
17 safely.

18 MS. CLAY: I would like to ask another question
19 or two and then open up to questions from the audience,
20 so if you have any that you're ready to ask.

21 We've talked a bit about insider threats, and I
22 know that the CSI FBI survey that recently came out, at
23 least the people that they surveyed say that 30 percent
24 of the threats are still coming from insiders. Is there

1 something that businesses can do to minimize or try to
2 better control that, the insider threat?

3 MR. WINKLER: Well, looking back about 15 years,
4 there was a great deal of discussion in the security
5 research and developing community about this kind of
6 question, and at that point in time research and
7 development in computer network security was essentially
8 funded either directly or indirectly through the DOD and
9 the intelligence community.

10 And when the question was posed to the business
11 community, it became evident that in fact the business
12 community had done something about this. It was called
13 the well formed transaction, and it simply amounted to
14 that no individual user of a system -- and if this was a
15 paper process and a paper process, no single individual
16 could both order, pay or approve and pay for a
17 fictitious item in order to gain off of that.

18 And the same really holds true for automated
19 systems, so, yes, it is possible to, first of all, limit
20 the damage that's potential and then the second thing is
21 of course intrusion detection, fraud detection and other
22 prone to error automated processes, and I can say that
23 legitimately because I was one of the first developers
24 of such an automated system. The number of false

1 positives and false negatives are really, really
2 difficult to manage.

3 But it doesn't mean that this is something that
4 fraud detection or intrusion technician are technologies
5 that should not be used but they should not be viewed as
6 the line of -- the only line of defense, so I think that
7 number 1 again it's an issue, how do you
8 characterize applications so that users of a minimum
9 amount of knowledge can use it, and two, how do you
10 rectify that with intrusion and fraud detection.

11 MS. CLAY: Frank, did you have a comment before
12 we go on?

13 MR. ZWILLINGER: Can I jump in on that? I spend
14 the majority of my time responding to insider
15 incidents. That's usually what I get called in to do,
16 and when I respond to them, I usually find three things
17 can go wrong in preventing the company from figuring out
18 what happened and prevent it from continuing loss.

19 One is they haven't turned their auditing on.
20 That is they didn't have enough storage space and
21 storage wasn't as cheap when they decided to put their
22 policies in place, so they weren't monitoring everything
23 that happened on their networks from an auditing point
24 of view or they weren't monitoring everything from a

1 legal point of view, that is, they didn't have policies
2 in place that said any time you do anything on the
3 network we're going to monitor and record it and if we
4 want to we can disclose it.

5 Sometimes it's a conscious choice. They don't
6 want to create an environment where everyone is being
7 monitored. More often it's not. The company wants to
8 have that, but they just never put it in place.

9 And there are tools out now that are just
10 wonderful at doing forensics like over the network. For
11 example Guidance Software and Cases just launched an
12 enterprise version where you can have an output on
13 anyone's computer system, and if you think there's some
14 kind of insider threat you run the output and image the
15 system immediately, and that's part of the growing
16 movement toward preventive forensics.

17 That is before you give someone a computer --
18 when a computer is turned on you image it before you
19 recycle and image it before you send it out so you know
20 what that employee did. You take an image every time
21 you're about to lay people off so you know what their
22 system looked like so they don't do any mischief in the
23 last couple days or if they did, you know what went on.

24 It's questionable whether they want to do this.

1 A lot of people in this room who are probably cringing
2 right now at these comments because they feel as an
3 employee perhaps that this is not the right type of
4 privacy model that they like, but it really does protect
5 the corporation so auditing, monitoring and preventive
6 forensics are ways you can limit drastically the insider
7 threat because if people know that you're doing that,
8 they're less likely to commit mischief, and if they do,
9 you can figure it out earlier and recover the losses, but
10 it's a question of tolerance for it.

11 MR. SOLLITTO: One really easy thing is to simply
12 separate responsibility for security from IT, having
13 people who are responsible for maintaining the security
14 network and protecting against bulk intrusions and
15 internal mischief, making sure they report separately up
16 the chain from those actually installing and maintaining the
17 network is an immediate -- that's a large source of
18 possibility for mischief.

19 MS. CLAY: Good points. Yes?

20 MR. KUO: I have -- Jimmy Kuo. I have a
21 two-part question, one the first part anybody can jump
22 in, and the second part is for Mr. Winkler primarily but
23 anybody else first.

24 How do you decide on which patch to apply

1 whenever you hear all these patches coming out? And the
2 second part is, Do you have any suggestions for how an
3 end user can ascertain the necessity of a particular
4 patch, assuming he even gets the information that a
5 patch is available, and perhaps do you, Mr. Winkler, do
6 any type of semiannual or annual roll up such as patches
7 so that they become easier?

8 We were talking earlier about the Stay Safe
9 Online campaign having semi annual campaigns to get
10 people to patch, and if we can get more companies to do
11 these semiannual roll ups so that we just have one thing
12 happen all at the same time.

13 MR. WINKLER: Right, first of all though, caveat of
14 my response, Sun is really not an end user consumer
15 computing client company, right? We sell servers
16 predominantly. We do sell workstations and start up
17 business because that's not our focus.

18 So our work station users are typically much
19 more sophisticated users than actual consumer or
20 business users, would be more on the side of engineering,
21 so my response as I think the only vendor on the panel
22 would be to identify which patches are necessary.

23 We're really focused on a different set of
24 users, and it's perhaps more difficult for an average

1 consumer using our products to determine whether or not
2 a patch would be appropriate.

3 But to answer the other question, the one about
4 roll ups, we do -- being a vendor we're in business to
5 sell things and so we sell new versions of our operating
6 system. Every about 18 months we have a new release,
7 and we have quarterly releases.

8 So it makes absolute sense to reinstall the
9 operating system on a quarterly or biannual basis not
10 just from the standpoint of rolling up patches but of
11 being able to access new functionality that's gone
12 through an 18 or 36 month studying period.

13 MR. KUO: Your standard is just to have
14 quarterly reinstalls of the operating system.

15 MR. WINKLER: No, updates of the operating
16 system. Most would involve patches as well that have
17 come with that.

18 MS. GOODENDORF: I would just say that we try
19 and do our patch management the way we do version
20 control management, and we're fortunate in that on our
21 mission critical systems, we have test environments
22 where we can test patches and test new versions before
23 we actually put them in production.

24 And some patches we frankly don't apply if they

1 don't seem to be relevant to us or provide any value to
2 us, so we do make decisions about which patches to
3 apply.

4 MS. CLAY: NIST does also maintain a database of
5 products and vulnerabilities and available patches.
6 However, it does make it very easy for you to go in and
7 click in a spot and have the -- and get to the right
8 patch, but you may want to know whether or not you want
9 that patch before you go to the database because it
10 doesn't help you decide whether or not you want to add
11 that patch, but it does sort of centralize things.

12 MS. CLAY: Yes, ma'am?

13 MS. LEVIN: Toby Levin. I'm concerned that
14 we're talking a lot about sort of a patch work of
15 patches, and my question really is -- I wasn't here this
16 morning to hear Dick Clarke's remarks but we have a
17 critical infrastructure problem that is at high risk
18 today, and I don't mean to be an alarmist, but it's
19 frightening when you think about our transportation,
20 telecom, financial sectors, all air transport could all
21 be brought down by some of the viruses and hacking and
22 technology issues that we talked about today.

23 So my concern is that what you're talking about
24 and what we talked about for the last few panels are

1 answers that could take decades to put into place, and I
2 don't think we have decades for that to happen, so my
3 question is: Y2K, an effort that was launched with a
4 very short time frame fully involving high levels of
5 leadership, government, industry played key roles
6 inputting out resources that even small businesses and
7 consumers could get help quickly, and we had very little
8 negative fall out from that effort.

9 My question is: Why can't we do a Y2K effort to
10 deal with these same technology security issues that
11 we're discussing now?

12 MR. REEDER: I would say facetiously since he's
13 my good friend because John Koskinen refuses to take
14 another task like he did on Y2K. A very good question,
15 a couple of reactions.

16 One, the level of problem we've been talking
17 about here is not the -- I don't think goes to the
18 question of protecting nuclear power plants or the power
19 grid or the telecommunication system which are indeed
20 for a variety of reasons subject to a higher level of
21 risk than other kinds of -- even notwithstanding its
22 economic importance to the economy and its stockholders,
23 the reservation systems of six Continents -- so we're
24 really talking about an order of magnitude different

1 problem although the nature of the problem is the same.

2 I have a problem with the Y2K metaphor because
3 unlike Y2K, I mean one we're not faced with a date
4 certain, and it's not clear that -- and I hate to use
5 the reference like the war on terrorism, it probably
6 will never be over. It's simply a problem of continuing
7 to mitigate and manage the risk which suggests
8 building into our processes and building into our
9 psyches, if you will, a whole different way of
10 approaching the problem than one could if there were
11 more waging a one-time push to get us through January 1
12 or to midnight of December 31, 1999.

13 The success of Y2K tends to -- we always like to
14 replicate our successes, but I think the problems are
15 not only in their scale but by their very nature
16 fundamentally different problems. We understood the
17 nature of the problem. We had a date certain by which
18 to fix it, and we went ahead and did that, and in fact
19 we -- and the sum of money involved was reasonably well
20 understood within two orders of magnitudes at least.

21 I think the problems are simply very, very
22 different.

23 MR. ZWILLINGER: They're different in part
24 because Y2K was a technology problem, and the threat of

1 attacks on the infrastructure is a people problem, and
2 the technologies used to help solve the problems, it
3 exacerbates the people problem and it's used to defend
4 against the people problem, but it's a people problem,
5 so it's a very, very different sort of situation.

6 MS. CLAY: Next.

7 MR. PALLER: Alan Paller from SANS again. This
8 panel had the end of the day job of pulling it all
9 together, and I didn't expect that to happen, but in
10 fact something really good came out of this and I want
11 to see if it's feasible.

12 All day we heard it's got to be easier, Scott
13 Charney said we have to have easier to use and we had
14 transparent security, invisible security, we have to
15 get securities out of being a problem and into being
16 easy. And you talked about having your test systems and
17 Frank you talked about having agreed upon benchmarks
18 this is what we want to install and, Vic, you talked
19 about having a server somewhere, and that everyone
20 downloads the current version of the server. I think
21 you know that like --

22 MR. WINKLER: I'm sorry, I like using servers
23 for lots of things.

24 MR. PALLER: Yes. Virginia uses some of your

1 servers. They tried awhile ago to install the operating
2 system. They had great success in installing the
3 operating system. They knew they had to get patches
4 down to protect against known vulnerabilities.

5 While they were downloading the patches they
6 were infected. They could not get the patches down in
7 time because there are so many automated attack programs
8 on the Internet, and I've been sitting here all day
9 trying to think of what's the general solution.

10 MR. WINKLER: JAVA, right? It was defined to
11 address exactly that.

12 MR. PALLER: Right. You install it on your
13 computer. You have Java on your computer, and while JAVA
14 goes and in fact gets the uninfected patches, some
15 hackers take your machine over. JAVA doesn't solve this
16 problem.

17 MR. WINKLER: To the traditional fat client that
18 happens. If you run a thin client --

19 MR. PALLER: This is the Microsoft/Sun
20 argument. Let's stay with the servers you sell now. In
21 the future you may sell non servers but right now --

22 MR. WINKLER: You're focusing the problem on the
23 operating systems, downloading operating systems.

24 MR. PALLER: You had this great idea which is

1 users have a version, this is a version. It's a safe
2 version, and we can all go get it if you need it, and
3 that would solve the problem if the safe version were
4 handled by the op staff and the op staff kept the
5 patches up to date.

6 My question is: How far are we from doing that
7 for consumers? Right now if I download or install a
8 copy of Windows 2000 server edition, odds are I won't
9 get patches down before it's infected with Code Red.
10 There's still 18,000 Code Reds.

11 So how far are we from getting you, Sun, to
12 deliver to the people who are willing to buy it an up to
13 date patch version of your system every day so that I
14 don't have to buy one that's four months old. It's the
15 end of the day. Let's keep it interesting.

16 MR. WINKLER: I think I used the term evolution
17 earlier, and we continue to evolve, right? It's a story
18 from the movie in the early 90s, but it is an issue, you
19 just described, circumscribed, a whole bunch of different
20 issues and there are a number of different answers for
21 different parts of those different problems.

22 One thing that consumers can do is they can
23 choose to buy a different platform from a different
24 vendor who is considered do be a niche player but whose

1 products interoperate completely with the ones that you
2 mentioned, and that I don't think work for that vendor,
3 but those products have been around for a long time and
4 all you have to do is think different, right, so when
5 you installed that operating system, it doesn't present
6 itself with hostile facing opportunities.

7 So it's been done. It has been done, and in
8 terms of when a vendor like Sun will deliver a highly
9 complex server product, that shouldn't be installed by
10 uneducated end users, the target installation should be
11 done by somebody who's trained.

12 We're freshly moving towards that fairly quickly
13 but to put it into perspective, our focus really is on a
14 different layer up in the cloud than the end user layer
15 despite the fact that we did design and build JAVA which
16 is the best computing solution for end users. Or so I
17 think.

18 MS. CLAY: Frank, did you want to make a quick
19 comment?

20 MR. REEDER: No.

21 MS. CLAY: Sorry.

22 MS. SAVAGE: I'm Jenny Savage from Capital One
23 Financial. We've been talking about standards for
24 software and various pieces of the security program that

1 we need, and I guess I'm wondering what the feeling is
2 on a little bit tougher standards on the people that you
3 hired to deal with the customers' information.

4 We as a company fingerprint everybody before
5 they touch customers' information, but not everybody
6 does that, and I guess I would like to know: Shouldn't
7 there be standards across the board for anybody that
8 touches customer information, as far as maybe checking
9 in to background, criminal history, that kind of thing?

10 MR. WINKLER: Absolutely, and in fact it's odd
11 but I had a VA conference last week and I was looking at
12 different booths and I have a little pamphlet here which
13 the -- I need my glasses. Otherwise I can't read. I
14 don't know who puts this out but if you can read it.

15 God bless you, it's entitled personal security
16 position sensitivity level designation process, and it
17 is really oriented towards exactly that and this is for
18 the government.

19 So clearly different positions require different
20 background checks, different ways of trust in those
21 individuals just like different systems in their
22 environment required different degrees of protection or
23 trust.

24 MS. GOODENDORF: I guess because I'm in the

1 hospitality industry, though, I would say that in hotels
2 and restaurants, throughout hospitality, consumers prefer
3 to use credit cards, and the nature of our industry is
4 such that to try to do background checks on all the
5 various people working at the front desk and working in
6 restaurants, that type thing, it just wouldn't be
7 manageable for us.

8 MR. ABRAMS: There are many cities that are full
9 of call centers that do consumer affairs similar to the
10 consumer affairs that you do at Capital One. I think
11 it's a great idea to only have the best, the brightest
12 the most honest.

13 The fact is for years losing 25 to 35 percent of
14 your workers each year was a bigger issue than making
15 sure that they were the best, the brightest and the most
16 honest. I think that absolutely we should have systems
17 to make sure that we have -- that we're indeed
18 eliminating the people problem. I think it's easier
19 said than done with the pressures we have in filling
20 positions.

21 MS. SAVAGE: I don't think it could be
22 completely eliminated but I think if you run a thorough
23 background check with anyone that's dealing with
24 customer's personal information could -- it could be a

1 future.

2 MR. ZWILLINGER: There's incredible reluctance
3 even when you've identified someone who is in some sort
4 of network management role who is a great employee from
5 a technical point of view to do anything to them, even
6 when you've caught them red handed doing something
7 improper on the networks.

8 I've been in positions where I would have to
9 produce evidence of this person is stealing from another
10 employee in the company and this is how they're doing
11 it. Yeah, but they're so good, isn't there something we
12 can do.

13 MS. SAVAGE; that's right, and I think that's
14 where we need standards. If we have standards, we could
15 have all the legal jargon where we need it that says if
16 you had this kind of criminal history or if you've been
17 fired from a job for this or that, you can't have a job
18 that is going to be dealing with customers'
19 information.

20 I wouldn't want somebody knowing my Social
21 Security -- the more -- if they've had any kind of shady
22 background at all, there's more chance that they're
23 going to do something with my information, so I think
24 that's as important as the software and packets and the

1 patches and all that.

2 MR. ABRAMS: Then you have to follow up and
3 indeed make sure your procedures are indeed followed.
4 It's not that many years ago that I was at the Federal
5 Reserve doing bank supervision regulation, and typically
6 it wasn't that the procedures weren't there, and the
7 policies weren't there.

8 It was, Well, you know, we couldn't afford for
9 them to take two weeks vacation or whatever was the
10 breach, so I think that again building the forensics
11 into the system I think is as important as doing -- yes,
12 you should do -- you should do what's prudent but it's
13 not always prudent to have, it's not always cost
14 effective to do a huge investigation of every single
15 employee.

16 MR. REEDER: I have nothing to add to the
17 substance, but I would add only two words of caution.
18 One, a labor market concern which I think has already
19 been raised and the other is a humanitarian concern. I
20 worked in an environment about ten blocks down the
21 street where we used to have a policy that anybody who
22 had ever used any controlled substance without
23 authorization was ineligible for employment until we
24 realized that we couldn't hire anybody under a certain

1 age. I offer that as caution number 1.

2 Caution number 2, and clearly I wouldn't argue
3 that we should employ pedophiles or individuals with
4 substantial histories of substance abuses as school bus
5 drivers, but people who have had -- who have in the past
6 engaged in activities that we might not approve of need
7 to be kept in society so I urge an awful lot of caution
8 apart from labor market considerations instantly
9 disqualifying large numbers of people.

10 MR. WINKLER: I have two names to drop, Ames and
11 Hansen, right? These are people who their organizations
12 are and yet --

13 MR. REEDER: That's the other quick one.

14 MR. SOLLITTO: One quick follow up on that as
15 well. One thing that I know we try and do at PayPal is,
16 how much information do employees really need. Does CRS
17 really need to know all 16 digits of your credit card to
18 help you?

19 No. Actually all I need is four numbers so you
20 can be sure you and he are talking about the same credit
21 card but you don't have to worry he has the entire
22 number so we do a number things beyond the vetting and
23 fingerprinting that we do and a variety of things to
24 also say, Let's try to minimize any possibility that

1 there could be.

2 Do we really need to have your street address, your
3 town, and your Zip Code or can we simply say are you
4 still on High School Way, and in fact that's one thing
5 we do is limit access to employees of information about
6 customers.

7 MS. CLAY: Good point s.

8 MR. AVILA: John Avila. This is primarily a
9 legal question so primarily directed to Mr. Zwillinge r.
10 What happens when preventative measures fail and there's
11 a compromise by a consumer enterprise? That disclosure
12 might occur either by intrusion, by an inadvertent
13 disclosure by the enterprise or by some internal
14 malfeasance?

15 What liability would apply in that situation?
16 Would it be a strict liability? Is there a form of
17 statutory liability? What sorts of damage would be
18 available -- limited to monetary loss by the consumer or
19 with emotional distress, would damages be available, punitive
20 damages, and finally what class of people would have
21 standing to assert a claim? Would it be limited to
22 consumers or for example would the banks that issued
23 credit cards have a claim for their losses as a result
24 of the misuse of consumer credit card?

1 MR. ZWILLINGER: How much time do you have?

2 MR. AVILA: How much time do you have? Finally
3 the question would be relating to the last question, I
4 believe there were a couple years an enterprise hired
5 prison inmates for their call centers and they got
6 access to credit card information and of course they
7 took it and used it for criminal purposes.

8 What kind of liability would be attached to that
9 kind of security procedure?

10 MR. ZWILLINGER: Without providing any specific
11 legal advice, let me give you a general sense of where
12 the liability doctrines are going in the area of this.
13 You obviously raised a lot of specific points.

14 For awhile there was no real net of liability in
15 the area. That is there were no standards to look to
16 for a negligence obligation. You have to find what
17 the -- what the standard of care is that you have a duty
18 to live up to and then you find a breach, and we were
19 sort of absent all of those things.

20 And now we're moving towards a much more
21 liability prone environment because there are standards
22 of care. There's the Gramm-Leach-Bliley Act. The
23 FTC finalized rules that came out on May 17. You
24 have the SEC rule regulation SP. You have HIPAA. You

1 have a bunch of places where there are regulated
2 entities that have obligations which will rapidly become
3 the standard of care.

4 But they're not very specific. They don't say,
5 your bylaws are configured this way, your policy has to
6 look like this, but it says you have to do a risk
7 assessment. You have to put in place a policy. I think
8 regulated entities will start being held liable or there
9 will be a move to hold them liable by those people to
10 whom they owe a duty.

11 And there aren't -- it wouldn't be every
12 third-party down the line, but here would be the
13 shareholders to whom they have a fiduciary duty. It would
14 be the customers to whom they have financial
15 information, but it's not there yet.

16 There's no third party liability, and where there's
17 been downstream liability efforts, there hasn't been any
18 published decisions. There's been the First Net versus
19 Nike case in Scotland where traffic was redirected and
20 they said Nike didn't manage their domain name well
21 enough so therefore I got a lot of your traffic and you
22 have to compensate me.

23 It's not there yet so who will be liable? At
24 first just regulated entities. Second after that people

1 who have the same type of information but aren't
2 regulated. Who will they be liable to? People who they
3 owe an existing duty. Shareholders? What will they be
4 liable for? All damages that are reasonably
5 foreseeable.

6 That doesn't mean necessarily every
7 consequence. I don't think that's where we're going to
8 start, but coming from a position of no liability moving
9 into the liability environment so it will start slowly and
10 go from there but you have to be concerned about
11 liability that you didn't have two or three years ago
12 and that's about it.

13 MS. CLAY: One last question.

14 MR. GARFINKEL: Really short. I'm a big
15 believer in out sourcing and I know the gentleman from
16 PayPal is also and I'm a customer of his, and I read on
17 the mailing list when they filed papers to go public
18 that they only have one data center which they said in
19 their papers to go public that the risk of the
20 catastrophic failure would put them out of business, and
21 so because I'm one of your customers, I would like to
22 know, do you have a second data center yet?

23 MR. SOLLITTO: We do. Unfortunately I believe
24 they're both within the same fault structure.

1 MR. GARFINKEL: So how do you vet the people you
2 out source to, not that I'm implying --

3 MR. SOLLITTO: I'm not sure who we out source to
4 today. There are very few data management systems left
5 in business now in California, but we're fortunately
6 going to be able to take care of a number of them. One of the things
7 we do --

8 MR. GARFINKEL: I meant how do customers --
9 let's refer to customers, consumers.

10 MR. SOLLITTO: How do customers or consumers
11 know the firms they're out sourcing to are taking
12 adequate precautions? Well, I guess that puts the
13 burden back on the consumer usually for education
14 information which perhaps can be a theme of this entire
15 event.

16 MR. GARFINKEL: The problem is I do not have a
17 lot of access to the information about the companies I could
18 use to make an informed decision. They say that's
19 proprietary information. We know about this. You put
20 it in your 10 K or whatever it was.

21 MR. SOLLITTO: S 1.

22 MR. GARFINKEL: There's so many other firms that
23 they do things with my data and I'm told to trust them.
24 VeriSign has taken the credit card on the same mailing

1 list. I read when you submit your credit card to
2 VeriSign, it doesn't get incented and there's many, many
3 cases where FTC maybe should be enforcing under the
4 advertising stuff that it used to go out to privacy but
5 there are many, many cases where they encourage out
6 sourcing. People we're out sourcing to are not acting
7 in an ethical or responsible manner.

8 MS. CLAY: Is there some place where businesses
9 can go now to either get a list of questions that they
10 should be asking of someone considering out sourcing or
11 where they can look at the business practices?

12 MR. SOLLITTO: I know a number of firms retain
13 research consultants and outside experts to help them in
14 their efforts to evaluate proper vendors. My firm looks
15 at Gardner Jupiter and others to help us in a variety of
16 research fronts which include vendor selection and
17 analysis so yes there are resources for businesses.

18 I think the point is well taken in that there
19 may be less resources available for consumers to either
20 get information or fully evaluate the company they're
21 choosing to use, but that's something that a good
22 business will do.

23 I know that just off point real quick many
24 customers always ask, Well, gosh, where is my money when

1 it's with you all, and so one of the things also we did
2 is put a little pop up on the front page, click here to
3 see the six banks your money is current sitting at
4 today.

5 And then it changes daily and they know that
6 information is there, so good businesses will recognize
7 that consumers are not like the Simpsons. Most
8 consumers want to know as much as they can so they can
9 make the evaluations they need and hopefully those
10 customers will be rewarded by usage, and that's frankly
11 how the market shortly will look.

12 MS. GOODENDORF: I would say something there
13 that I think there's a predicament when you're running
14 an information security program in a company like I am
15 which is that while I want to reassure consumers, I
16 don't want to give clues to the bad guys on the
17 particulars of how we're arranged and what platforms we
18 have and so forth.

19 And I kind of wish that we could have something
20 that would resemble the Good Housekeeping seal of
21 approval, that we could have something that would be a
22 standard or an independent kind of a mark to tell
23 consumers, Okay, we meet this criteria or these
24 standards without giving them the particulars of how we

1 perform our security.

2 MR. ZWILLINGER: There are certification
3 authorities. I mean, there are three I can think of
4 right now that do it, network information security
5 systems, but I think there will be a move with the new
6 standards like in Europe with British Standard 7799.
7 There will be a lot of certification authorities who
8 will give you your good housekeeping approval, and
9 Foundstone Internet Security System and TRUSTe and other
10 people will do it.

11 MS. CLAY: Frank? Okay. You kept fooling me,
12 Frank.

13 Well, that's all we have time for. I think this
14 was a very good discussion, and again I just want to say
15 that the panelists are going to provide Mark with some
16 resources to put up on the FTC web site so you can get
17 more detail on some of the things we talked about.
18 Thank you again.

19 MR. EICHORN: Just a moment here. I want to
20 introduce Howard Beales for the close, if you could get
21 settled for one moment.

22 MR. BEALES: I promise not to keep you very
23 long, but before we close I would like to thank the
24 panelists for speaking about information security. I'm

1 very impressed with the knowledge base we've assembled
2 here, and I hope we'll be able to continue to tap into
3 that expertise as we go forward.

4 I would like to make a few observations on some
5 of the themes that I've seen emerge from the first day
6 of the workshop. There's more of the workshop tomorrow,
7 but I think we can look at the panels today as focusing
8 on where we are now and what businesses and consumers
9 can do about it today.

10 Tomorrow, fittingly, we'll be looking at what can
11 be done tomorrow, what approaches or ideas or movements
12 are beginning to develop that may take a little longer
13 to happen and may make things a little better.

14 Here's what I think we've learned so far. Our
15 first panel made clear that there's a growing number of
16 threats out there of different varieties and that
17 technology advances like broadband, Instant Messaging,
18 and wireless have created new areas of vulnerability.

19 The potential threats are daunting. As a
20 technical matter, securing one system from a
21 sophisticated determined hacker is extremely difficult,
22 but there are things that knowledgeable consumers can do
23 to significantly decrease their exposure to the most
24 common security risks.

1 Some of these steps involve simple good security
2 practices and little or no expense. For example, you
3 can physically disconnect a broadband Internet
4 connection when it's not in use or not open email
5 attachments when you don't know what they are.

6 Other steps take more effort and involve
7 monitoring threats and updating or patching accordingly,
8 and as we learned today there's a wide variety of
9 products and services available to assist consumers in
10 reducing their risks.

11 We've also heard about some imaginative methods
12 for delivering these products to consumers so
13 maintaining one's security is a little bit easier.
14 We've learned that although there's a lot of people here
15 today who are working to educate consumers, there are a
16 lot of consumers who don't know the dangers or what
17 options they have to reduce the risk or why security is
18 important.

19 As a result, many people do not take simple
20 steps to safeguard their own security and their own
21 information. More consumer education would be helpful
22 in getting the message out. From the business
23 perspective, managing security is a constant process
24 that involves frequent trade-offs between considerations

1 like security and privacy, security and convenience and
2 security and cost to name a few.

3 A vigilant chief security officer or chief
4 information officer, sometimes with the help of outside
5 consultants or managed security services, can do a lot
6 to reduce the risks by planning, analyzing, and managing
7 risks, and by responding quickly to incidents when they
8 occur.

9 That's where we are at this point. Tune in
10 tomorrow.

11 (Whereupon, at 5:05 p.m., the workshop was
12 adjourned.)

13
14
15
16
17
18
19
20
21
22
23
24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

C E R T I F I C A T I O N O F R E P O R T E R

CASE TITLE: WORKSHOP
HEARING DATE: MAY 20, 2002

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: JUNE 4, 2002

DEBRA L. MAHEUX

C E R T I F I C A T I O N O F P R O O F R E A D E R

For The Record, Inc.
Waldorf, Maryland
(301)870-8025

1 I HEREBY CERTIFY that I proofread the transcript
2 for accuracy in spelling, hyphenation, punctuation and
3 format.

4

5

DIANE QUADE

6

7